Configuring Bridging Services

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114060 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Configuring Bridging Services

About This Guide

Before You Begin xvii
Conventions xviii
Acronyms xix
Ordering Bay Networks Publications xx

Technical Support and Online Services

Bay Networks Customer Service xxii
Bay Networks Information Services xxiii
World Wide Web xxiii
Customer Service FTP xxiii
Support Source CD xxiv
CompuServe xxiv
InfoFACTS xxv
How to Get Help xxv

Chapter 1
Using Transparent Bridge Services

Transparent Bridge Overview 1-1
How the Bridge Works 1-2
The Translation Process 1-3
Spanning Tree Algorithm 1-8
Filtering Frames 1-14
Enabling Bridge Service 1-15
Enabling Bridge Service on an Interface 1-15
Enabling Spanning Tree on an Interface 1-15
Editing Bridge Parameters 1-18
Editing Bridge Global Parameters 1-19

Bridge Global Parameter Descriptions 1-20
Editing Bridge Interface Parameters 1-22
Bridge Interface Parameter Descriptions 1-23
Editing Spanning Tree Global Parameters 1-24
Spanning Tree Global Parameter Descriptions 1-25
Editing Spanning Tree Interface Parameters 1-29
Spanning Tree Interface Parameter Descriptions 1-30
Flushing the Forwarding Table 1-32
Deleting the Bridge and Spanning Tree from the Router 1-32

Chapter 2
Using Source Routing Bridge Services

Source Routing Overview 2-1
How Source Routing Differs from Transparent Bridging 2-2
How Endstations on a Source Routing Network Discover Routes 2-2
All-Paths Broadcast Routing 2-2
Spanning Tree Broadcast Routing 2-3
Specific Routing 2-4
Source Routing over IP Networks 2-4
How IP Encapsulation Works 2-5
IP Encapsulation Features 2-8
Source Route Endstation Support 2-9
How the Bay Networks Source Routing Bridge Works 2-10
Source Routing across a Token Ring Network 2-11
How the Source Routing Bridge Handles Explorer Frames 2-11
How the Source Routing Bridge Handles Specifically Routed Frames 2-14
Source Routing across an IP Network 2-17
IP Encapsulation Guidelines 2-21
Source Routing over Frame Relay Networks 2-21
Source Routing over FDDI 2-21
For More Information about Source Routing 2-22
Implementation Notes 2-22
Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs 2-22
Bridge ID 2-22
Internal LAN ID 2-24
Group LAN ID 2-24

Configuring IP Encapsulation Support 2-24
Enabling Source Routing Services 2-25
Enabling Source Routing Services on an Interface 2-26
Enabling Source Routing Spanning Tree Service on an Interface 2-30
Editing Source Routing Parameters 2-33
Editing Source Routing Global Parameters 2-33
Source Routing Global Parameter Descriptions 2-34
Editing Source Routing Interface Parameters 2-38
Source Routing Interface Parameter Descriptions 2-40
Adding or Deleting a Bridge ID on the Bridge Entry List 2-45
Adding a Bridge Entry to the Bridge Entry List 2-45
Source Routing Bridge ID Parameter Description 2-46
Deleting a Bridge Entry from the Bridge Entry List 2-47
Adding or Deleting an IP Address on the IP Explorer Address List 2-47
Adding an IP Explorer Address to the IP Explorer Address List 2-48
IP Explorer Address Parameter Description 2-49
Deleting an IP Explorer Address 2-49
Editing Source Route Spanning Tree Global Parameters 2-50
Source Route Spanning Tree Global Parameter Descriptions 2-51
Editing Source Route Spanning Tree Interface Parameters 2-56
Source Route Spanning Tree Interface Parameter Descriptions 2-57
Deleting Source Routing from the Router 2-58

Chapter 3
Using NetBIOS Services

NetBIOS Overview 3-1
NetBIOS Names 3-1
Registering Station Names 3-2
Establishing Sessions 3-3
Sessionless Communication 3-4
Broadcast Reduction 3-4
Name Caching 3-5
Client Name Caching 3-5
Server Name Caching 3-6
Datagram RIF Caching 3-6
Query Caching 3-7

Cache Lookup 3-8
Cache Aging 3-8
Statically Configured NetBIOS Names 3-9
Implementation Notes 3-9
Topologies 3-9
Spanning Tree Topology 3-9
Other Topologies 3-10
NetBIOS Caches 3-10
Enabling NetBIOS Services 3-10
Editing NetBIOS Parameters 3-11
Editing NetBIOS Global Parameters 3-13
NetBIOS Global Parameter Descriptions 3-14
Editing NetBIOS Interface Parameters 3-20
NetBIOS Interface Parameter Descriptions 3-21
Using Statically Configured NetBIOS Clients and Servers 3-22
Adding a Statically Configured NetBIOS Client or Server 3-23
Static Name Parameter Descriptions 3-24
Editing Statically Configured NetBIOS Clients and Servers 3-26
NetBIOS Static List Parameter Descriptions 3-26
Deleting a Statically Configured NetBIOS Name 3-28

Chapter 4
Using Translation Bridge Services

Translation Bridge Overview 4-1
Databases 4-2
Forwarding Database 4-2
Route Information Field Database 4-2
Database Aging Mechanism 4-2
Bridge Operations 4-3
SR Operations 4-3
TB Operations 4-4
TB to SR Challenges 4-5
Frame Format Selection 4-6
Frame Lengths 4-6
MAC Address Formats 4-6
LAN Speeds 4-7

Implementation Notes 4-7
Protocols Supported 4-7
Interfaces Supported 4-7
Loop-Free Operation 4-8
Physically Disabling Loops 4-8
Using the Spanning Tree Protocol 4-9
Procedure for Configuring the Translation Bridge on Your Network 4-11
Enabling Source Routing Translate/LB Service 4-12
Creating the Translation Bridge 4-14
Editing Translation Bridge Parameters 4-15
Editing Translation Bridge Global Parameters 4-15
Translation Bridge Global Parameter Descriptions 4-16
Editing Translation Bridge MAC Address Conversions 4-21
Adding an Address Mapping 4-21
Translation Bridge Address Mapping Parameter Descriptions 4-23
Deleting an Address Mapping 4-23
Editing Translation Bridge Station Type 4-24
Adding a New Address to the Station List 4-24
Translation Bridge Ethernet Address Mapping Parameter Descriptions 4-25
Deleting a Station 4-26
Deleting the Translation Bridge from the Router 4-26

Chapter 5
Using Native Mode LAN Services

Native Mode LAN Overview 5-1
Defining a Closed User Group 5-3
Implementation Notes 5-3
Defining a Closed User Group That Permits Overlapping Network Traffic 5-4
Controlling NML Traffic on a Network Trunk 5-4
Enabling NML Services 5-5
Editing NML Parameters 5-6
Editing NML Interface Parameters 5-7
NML Interface Parameter Descriptions 5-8
Assigning an Access List to a Port 5-11
NML Add Security Range Parameters 5-13
Enabling Ranges 5-14

NML Range Enable Parameter Description 5-16
Deleting NML from the Router 5-16

Appendix A
Site Manager Default Settings

Appendix B
Components of a Source Route Frame

802.5 Physical Header B-1
Routing Information Field (RIF) B-2
Routing Control B-2
Type of Frame B-3
Length B-3
Direction Bit B-3
Frame Size Bits B-3
Routing Designators B-4

Index

Figures

Figure 1-1. Forwarding Table Update 1-2
Figure 1-2. RFC 1042 Encapsulation 1-4
Figure 1-3. Bridge Tunnel Service Encapsulation 1-4
Figure 1-4. Ethernet to FDDI Translation 1-5
Figure 1-5. FDDI to Ethernet Translation 1-6
Figure 1-6. Ethernet/802.3 to FDDI Translation 1-7
Figure 1-7. AppleTalk ARP (Originating on FDDI) to 802.3 Translation 1-8
Figure 1-8. Parallel Bridge Topology 1-9
Figure 1-9. Root Port Determination (Equal Path Costs) 1-11
Figure 1-10. Root Port Determination (Equal Path Costs and Root Interface Priorities) 1-12
Figure 1-11. Spanning Tree (Loop-Free) Logical Topology 1-13
Figure 1-12. Inefficient Spanning Tree Topology 1-14
Figure 1-13. Spanning Tree Autoconfiguration Window 1-17
Figure 1-14. Configuration Manager Window 1-19
Figure 1-15. Edit Bridge Global Parameters Window 1-20
Figure 1-16. Bridge Interfaces Window 1-23
Figure 1-17. Edit Spanning Tree Global Parameters Window 1-25
Figure 1-18. Spanning Tree Interfaces Window 1-30
Figure 2-1. Source Routing Network 2-1
Figure 2-2. Source Routing Designator 2-3
Figure 2-3. Route Discovery 2-4
Figure 2-4. Source Routing over an IP Network 2-6
Figure 2-5. Examining the RIF Field of an SRF 2-7
Figure 2-6. IP Routers Source Routing across a Token Ring Network 2-10
Figure 2-7. Tracking an Explorer Frame 2-11
Figure 2-8. Structure of an Explorer Frame 2-13
Figure 2-9. Tracking a Specifically Routed Frame from ES2 to ES1 2-14
Figure 2-10. Structure of a Specifically Routed Frame from ES2 to ES1 2-16

Figure 2-11. Tracking an IP-Encapsulated Frame from ES1 to ES2 2-17
Figure 2-12. Structure of an IP-Encapsulated Frame from ES1 to ES2 2-19
Figure 2-13. Parallel Operation 2-23
Figure 2-14. Edit Source Routing Global Parameters Window 2-27
Figure 2-15. SR Interface List Window 2-29
Figure 2-16. Source Route Spanning Tree Autoconfiguration Window 2-31
Figure 2-17. Configuration Manager Window 2-33
Figure 2-18. Edit Source Routing Global Parameters Window 2-34
Figure 2-19. SR Interface List Window 2-39
Figure 2-20. Source Routing Bridge IDs Window 2-45
Figure 2-21. Add Bridge ID Window 2-46
Figure 2-22. Source Routing Bridge IP Explorer Addresses Window 2-48
Figure 2-23. Add Source Routing Explorer IP Address Window 2-48
Figure 2-24. Edit Source Route Spanning Tree Global Parameters Window 2-50
Figure 2-25. Source Route Spanning Tree Interface List Window 2-56
Figure 3-1. Configuration Manager Window 3-12
Figure 3-2. Edit Source Routing Global Parameters Window 3-13
Figure 3-3. SR Interface List Window 3-20
Figure 3-4. NetBIOS Static List Window 3-23
Figure 3-5. NetBIOS Window 3-24
Figure 4-1. Network Configuration with Potential Loop 4-8
Figure 4-2. Spanning Tree with Translation Bridging 4-10
Figure 4-3. Edit Translation Bridge Global Parameters Window 4-13
Figure 4-4. Configuration Manager Window 4-14
Figure 4-5. Edit Translation Bridge Global Parameters Window 4-16
Figure 4-6. Address Mapping List Window 4-22
Figure 4-7. Translation Bridge Address Mapping Window 4-22
Figure 4-8. Ethernet Station Type List Window 4-24
Figure 4-9. Translation Bridge Address Mapping Window 4-25
Figure 5-1. NML Closed User Groups 5-2
Figure 5-2. Edit NML Interface Window 5-5
Figure 5-3. Configuration Manager Window 5-7
Figure 5-4. NML Interfaces Window 5-8
Figure 5-5. NML Filters Window 5-12
Figure 5-6. NML Add Security Range Window 5-12

Figure 5-7. Circuit List Window 5-14
Figure 5-8. Circuit Definition Window 5-15
Figure B-1. Fields in a Source Route Frame B-1
Figure B-2. Components of the RIF B-2

Tables

Table A-1. Transparent Bridge Global Parameters A-1
Table A-2. Transparent Bridge Interface Parameters A-1
Table A-3. Spanning Tree Global Parameters A-2
Table A-4. Spanning Tree Interface Parameters A-2
Table A-5. Source Routing Global Parameters A-3
Table A-6. Source Routing Interface Parameters A-4
Table A-7. Source Routing Bridge ID Parameter A-4
Table A-8. IP Explorer Address Parameter A-4
Table A-9. Source Route Spanning Tree Global Parameters A-5
Table A-10. Source Route Spanning Tree Interface Parameters A-5
Table A-11. NetBIOS Global Parameters A-6
Table A-12. NetBIOS Interface Parameters A-6
Table A-13. NetBIOS Static Name Parameters A-7
Table A-14. Translation Bridge Global Parameters A-7
Table A-15. Translation Bridge Address Mapping Parameters A-7
Table A-16. Translation Bridge Ethernet Address Mapping Parameters A-8
Table A-17. NML Interface Parameters A-8
Table A-18. NML Add Security Range Parameters A-8
Table A-19. NML Range Enable Parameters A-8
Table B-1. Frame Size Bits B-3

About This Guide

If you are responsible for configuring and managing Bay Networks™ routers, you should read this guide to learn how to customize Bay Networks router software for bridging services.

This guide offers details on configuring

- Transparent bridging services (Chapter 1)
- Source routing bridge services (Chapter 2)
- NetBIOS services (Chapter 3)
- Translation bridge services (Chapter 4)
- Native mode LAN (NML) services (Chapter 5)

Before You Begin

Before using this guide, complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers and BNX Platforms*, *Connecting BayStack AN and ANH Systems to a Network*, or *Connecting ASN Routers and BNX Platforms to a Network)*.
- Make sure that you are running the latest version of Bay Networks Site Manager and router software (refer to *Upgrading Routers from Version 7–10.xx to Version 11.0)*.
- Create and save a configuration file that has at least one bridging interface (refer to *Configuring Routers*).
- Retrieve the configuration file in local, remote, or dynamic mode.
- Reboot the router with the configuration file.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

APE	all-paths explorer frame
ARE	all-routes explorer frame
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CUGID	closed user group ID
DA	destination address
DLCI	data link connection identifier
DLSw	data link switching
DSAP	destination service access point
FCS	frame check sequence
FDDI	Fiber Distributed Data Interface
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPX	Internet Packet Exchange
LLC	logical link control
LNM	LAN Network Manager
MAC	media access control
MIB	Management Information Base
MTU	Maximum Transmission Unit
NetBIOS	Network Basic Input/Output System
NML	Native Mode LAN
OUI	organizationally unique identifier
PPP	Point-to-Point Protocol
RFC	Request for Comments
RIF	Routing Information Field
SA	source address
SAP	service access point
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
SR	source routing
SRF	specifically routed frame

SSAP	session service access point
STE	spanning tree explorer frame
TB	transparent bridging
XNS	Xerox Network System

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Using Transparent Bridge Services

This chapter contains information on the following topics:

- The transparent bridge, including an overview of the transparent bridge and details on how the spanning tree algorithm works
- Enabling bridge service and spanning tree on an interface
- Transparent bridge parameters, including information on how to edit the parameters using Configuration Manager
- Deleting the bridge and spanning tree from the router

Transparent Bridge Overview

Transparent bridges are data-link layer relay devices that connect two or more networks. They use media access control (MAC) source and destination addresses to relay frames between connected networks.

Note: We use the terms *bridge* and *transparent bridge* interchangeably throughout this chapter.

The transparent bridge provides three primary services:

- Learns the addresses of endstations on connected networks
- Forwards or drops frames based on knowledge it acquires about endstation addresses or user-configured filters
- Ensures a loop-free topology throughout the extended network, using the spanning tree algorithm

A transparent bridge also provides some translation services, converting frames for bridging between Ethernet/802.3 LANs and Fiber Distributed Data Interface (FDDI) LANs. Refer to The Translation Process later in this chapter for details on translation services.

How the Bridge Works

The bridge receives and examines every frame transmitted on the networks to which it is attached. It learns endstation addresses by reading the source address of the endstation that transmitted the frame and noting which LAN interface received the frame. The bridge enters this information into a data structure called the *forwarding table*, which the bridge constantly updates.

For example, in Figure 1-1, if Node 2 transmits a frame onto the network for the first time, the bridge receives the frame and makes an update to its forwarding table. The bridge notes that Node 2 is in the direction of LAN A.

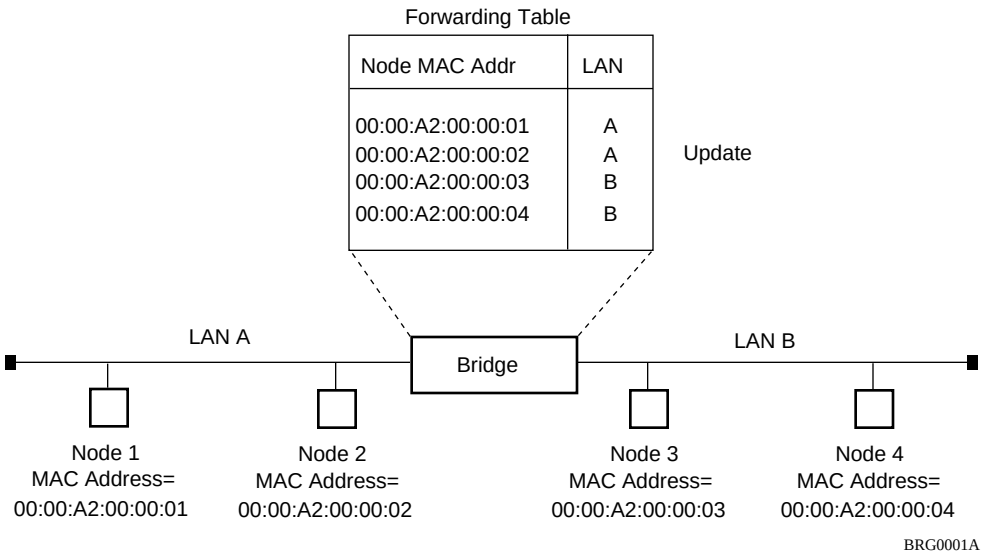


Figure 1-1. Forwarding Table Update

The bridge then forwards (relays to another network) or drops (discards) the frame based on the forwarding table entries. When the bridge receives a frame, it compares the frame's destination address with addresses in the forwarding table. One of these situations results:

- If the frame's destination address is on the same LAN as its source address, the bridge discards the frame; all nodes on that LAN already received this frame.
- If the frame's destination address is on a different LAN than its source address, the bridge *forwards* the frame to that LAN.
- If there is no match for the frame's destination address in the forwarding table, the bridge forwards the frame to all networks except the one that received the frame. This is called flooding.
- If the frame is destined for the bridge (for example, a spanning tree frame), the bridge forwards the frame to the appropriate bridge entity and processes it internally.

Note: If a frame is forwarded or flooded to a LAN using a *different* data-link level protocol, the bridge translates the frame to the appropriate frame format before transmission.

The Translation Process

The transparent bridge translates frames for bridging between Ethernet/802.3 LANs and FDDI LANs. When the transparent bridge receives Ethernet/802.3 frames destined for an FDDI LAN, it reformats those frames to the FDDI MAC frame format. The transparent bridge sets the original MAC frame type in the logical link control (LLC) header. Therefore, if the frame passes through a second, FDDI-to-Ethernet/802.3 bridge, that bridge can translate the frame back to its original format.

The bridge translates all Ethernet MAC frames to FDDI MAC and IEEE 802.2 LLC/Subnetwork Access Protocol (SNAP) encapsulation, as specified by RFC 1042. Protocols that adhere to RFC 1042 include DECnet Phase IV, Novell, AppleTalk Phase I and II, Xerox Network System (XNS), Internet Package Exchange (IPX), and Internet Protocol (IP).

Figure 1-2 shows the format and values of the LLC and SNAP headers of these frames after translation.

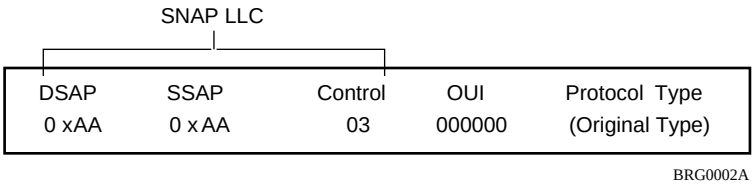


Figure 1-2. RFC 1042 Encapsulation

AppleTalk Address Resolution Protocol (ARP) frames (Ethernet frames with a protocol type equal to 80F3) require special translation by the Bridge Tunnel Service.

Figure 1-3 illustrates the LLC and SNAP headers of the AppleTalk ARP outbound frame after the Bridge Tunnel Service translation.

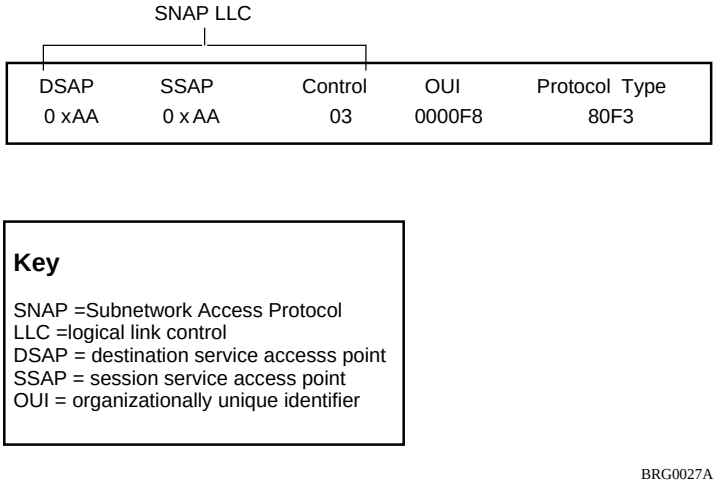
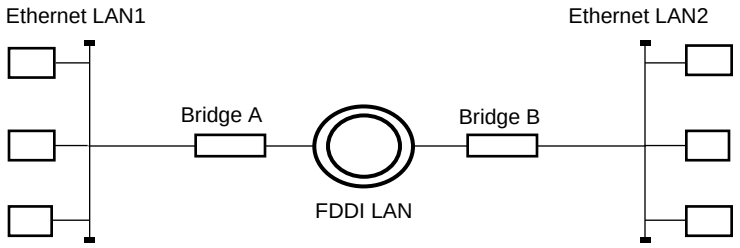


Figure 1-3. Bridge Tunnel Service Encapsulation

The bridge translates all IEEE 802.2 LLC frames by removing the length field. Protocols in this category include AppleTalk Phase 2, Novell Proprietary, and IP.

Figures 1-4 and 1-6 illustrate different LAN configurations and show how Bridge A translates different types of frames originating on LAN 1 for transmission across the FDDI LAN. Figure 1-5 shows how Bridge B translates frames transmitted from the FDDI LAN to LAN 2.



Ethernet to FDDI Translation

From Ethernet LAN

DA	SA	TYPE =80F3	DATA	FCS

Through Bridge A to FDDI LAN

DA	SA	SNAP LLC			OUI			TYPE =80F3	DATA	FCS
		AA	AA	03	00	00	00			

Bridge A

- Extracts addressing information from the Ethernet header.
- Incorporates address information into newly generated FDDI MAC header.
- Encapsulates Ethernet data according to RFC 1042.
- Recalculates frame check sequence (FCS).

Ethernet (AppleTalk ARP) to FDDI Translation

From Ethernet LAN

DA	SA	TYPE =80F3	DATA	FCS

Through Bridge A to FDDI LAN

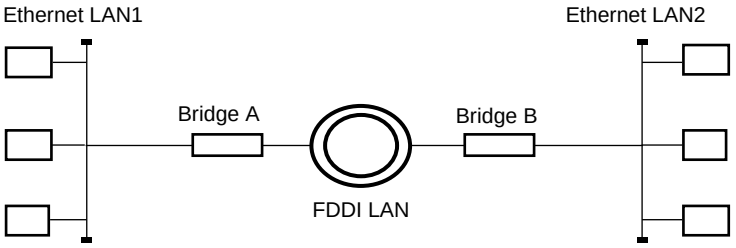
DA	SA	SNAP LLC			OUI			TYPE =80F3	DATA	FCS
		AA	AA	03	00	00	F8			

Bridge A

- Extracts addressing information from the Ethernet header.
- Incorporates address information into newly generated FDDI MAC header.
- Encapsulates Ethernet data within IEEE 802.2H-defined SNAP header that has an organizationally unique identifier (OUI) of 0000F8.
- Recalculates (FCS).

BRG0003A

Figure 1-4. Ethernet to FDDI Translation



FDDI to Ethernet Translation

From FDDI LAN

DA	SA	SNAP LLC			OUI			TYPE	DATA	FCS
		AA	AA	03	00	00	00	=80F3		

Through Bridge B to Ethernet LAN

DA	SA	TYPE =80F3	DATA	FCS

Bridge B

- Extracts addressing information from the FDDI header.
- Incorporates address information into newly generated Ethernet MAC header.
- Removes RFC 1042 from Ethernet data.
- Recalculates frame check sequence (FCS).

FDDI to Ethernet (AppleTalk ARP) Translation

From FDDI LAN

DA	SA	SNAP LLC			OUI			TYPE	DATA	FCS
		AA	AA	03	00	00	F8	=80F3		

Through Bridge B to Ethernet LAN

DA	SA	TYPE =80F3	DATA	FCS

Bridge B

- Extracts addressing information from the FDDI header.
- Incorporates address information into newly generated Ethernet MAC header.
- Removes Ethernet data from an IEEE 802.2H-defined SNAP header that has an organizationally unique identifier (OUI) of 0000F8.
- Recalculates FCS.

BRG0028A

Figure 1-5. FDDI to Ethernet Translation

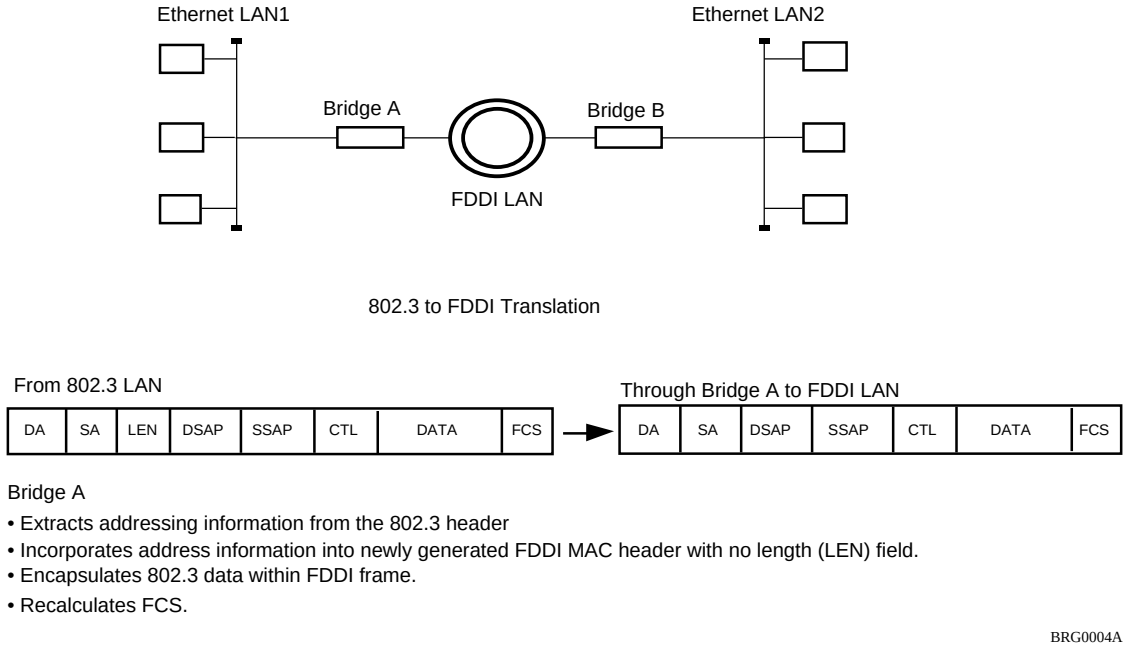


Figure 1-6. Ethernet/802.3 to FDDI Translation

The translation process from the FDDI LAN to Ethernet/802.3 LAN (the process Bridge B performs in Figures 1-5 and 1-6) is a mirror image of the translation process occurring on Bridge A, with one exception: the bridge translates an AppleTalk ARP frame that originates on the FDDI LAN and is destined for an Ethernet/802.3 LAN as shown in Figure 1-7.

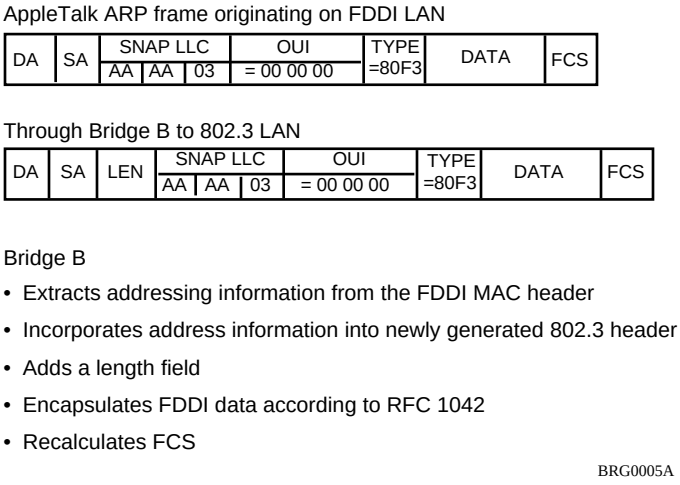


Figure 1-7. AppleTalk ARP (Originating on FDDI) to 802.3 Translation

Spanning Tree Algorithm

The spanning tree algorithm ensures the existence of a loop-free topology in networks that contain parallel bridges. (Refer to *Source Routing Appendix to IEEE Standard 802.1d Media Access Control (MAC) Bridges* for details on the spanning tree algorithm.) A loop occurs when there are alternate routes between hosts. If there is a loop in an extended network, bridges may forward traffic indefinitely, which can result in increased traffic and degradation in network performance.

Figure 1-8 shows an example of a network containing a loop: two parallel bridges, Bridge 1 and Bridge 2, connect LANs A and B.

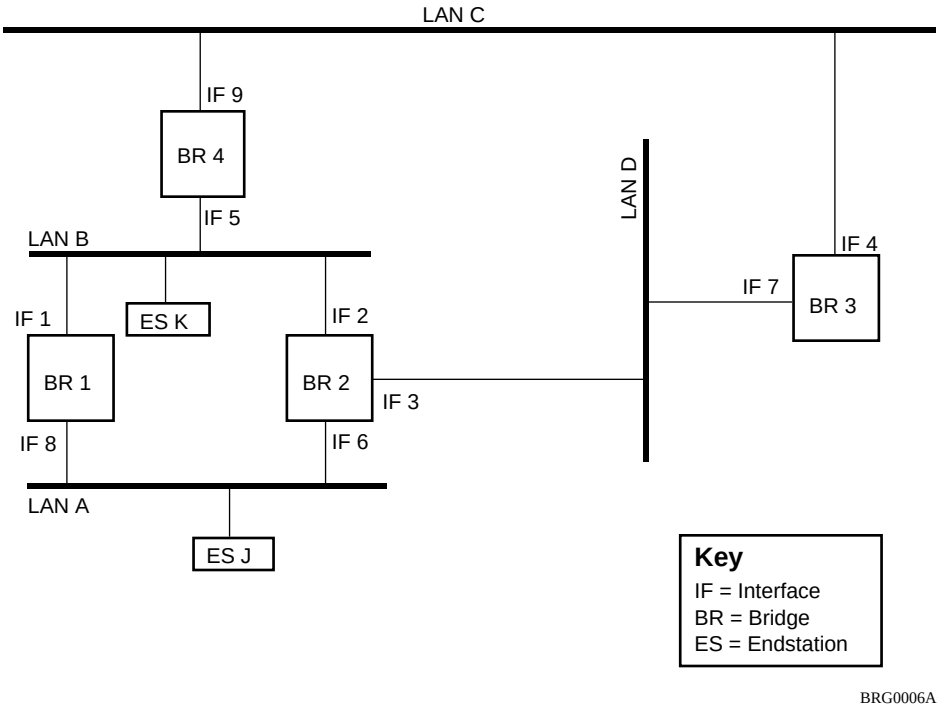


Figure 1-8. Parallel Bridge Topology

When Endstation J initially sends a frame to Endstation K, both Bridge 1 and Bridge 2 read the frame. Since this is the first frame sent between J and K, there is no forwarding table entry for J or K on either of the bridges. Each bridge updates its forwarding table to indicate that Endstation J is in the direction of LAN A. Then, each bridge floods the frame: Bridge 1 forwards the frame over Interface 1 and Bridge 2 forwards the frame over Interface 2. Bridge 2 also forwards the frame over Interface 3; however, to simplify the example, we do not trace this frame.

Next, Endstation K receives two copies of the frame, resulting in an inefficient use of the available bandwidth. More serious, however, is the effect of duplicate frames on the two bridges. The frame flooded by Bridge 1 onto Interface 1 is ultimately read by Bridge 2 on Interface 2. When Bridge 2 reads this frame, it updates its forwarding table to indicate that Endstation J is in the direction of LAN B. Similarly, Bridge 1 reads the frame flooded by Bridge 2 and updates its forwarding table to show that Endstation J is in the direction of LAN B. Consequently, the forwarding tables of both bridges are now corrupted and neither bridge can properly forward a frame to Endstation J.

You can avoid this problem by implementing the spanning tree algorithm, which produces a logical tree topology out of any arrangement of bridges. The result is that a single path exists between any two endstations on an extended network. The spanning tree algorithm also provides a high degree of fault tolerance. It allows the network to automatically reconfigure the spanning tree topology if there is a bridge or data-path failure.

The spanning tree algorithm requires five values to derive the spanning tree topology. The first, a multicast address specifying all bridges on the extended network, is media-dependent and is automatically determined by the software. You assign the remaining four values, which are

- Network-unique identifier for each bridge on the extended network
- Unique identifier for each bridge/LAN interface (called a port)
- Priority specifying the relative priority of each port
- Cost for each port

After you assign these values, bridges multicast and process the formatted frames (called Bridge Protocol Data Units, or BPDUs) to derive a single loop-free topology throughout the extended network. The bridges exchange BPDU frames quickly, minimizing the time that service is unavailable between hosts.

In constructing a loop-free topology, the bridges within the extended network follow these steps:

1. **Elect a root bridge.**

   The bridge with the lowest priority value becomes the root bridge and serves as the root of the loop-free topology. If priority values are equal, the bridge with the lowest bridge MAC address becomes the root bridge.

2. **Determine path costs.**

   The path cost is the cost of the path to the root bridge offered by each bridge port.

3. **Select a root port and elect a designated bridge on each LAN.**

   Each bridge designates the port that offers the lowest-cost path to the root bridge as the root port. In the event of equal path costs, the bridge examines the paths' interfaces to the root bridge. The port (interface) of the path with the lowest interface priority to the root bridge becomes the root port. For example, Figure 1-9 shows how Bridge A determines its root port.

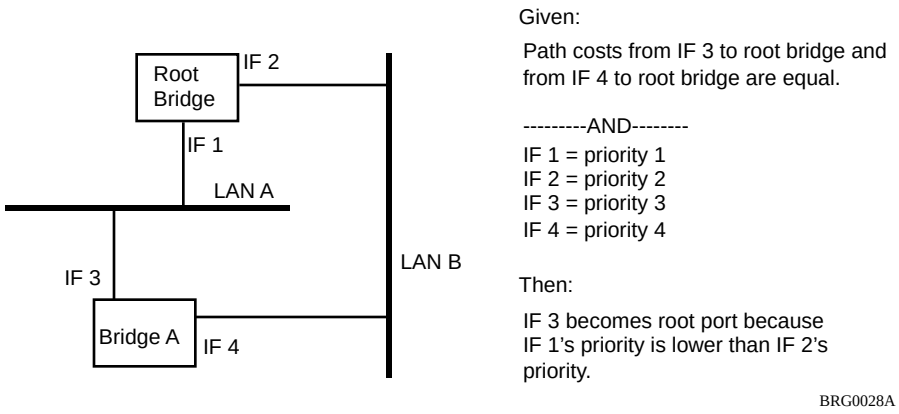

Root Bridge
IF 2
IF 1
LAN A
IF 3
LAN B
Bridge A
IF 4
Given:
Path costs from IF 3 to root bridge and from IF 4 to root bridge are equal.
---------AND--------
IF 1 = priority 1
IF 2 = priority 2
IF 3 = priority 3
IF 4 = priority 4
Then:
IF 3 becomes root port because IF 1's priority is lower than IF 2's priority.
BRG0028A

Figure 1-9. Root Port Determination (Equal Path Costs)

If the paths' interfaces to the root bridge are also equal, then the root port is the port on the bridge with the lowest priority value (Figure 1-10).

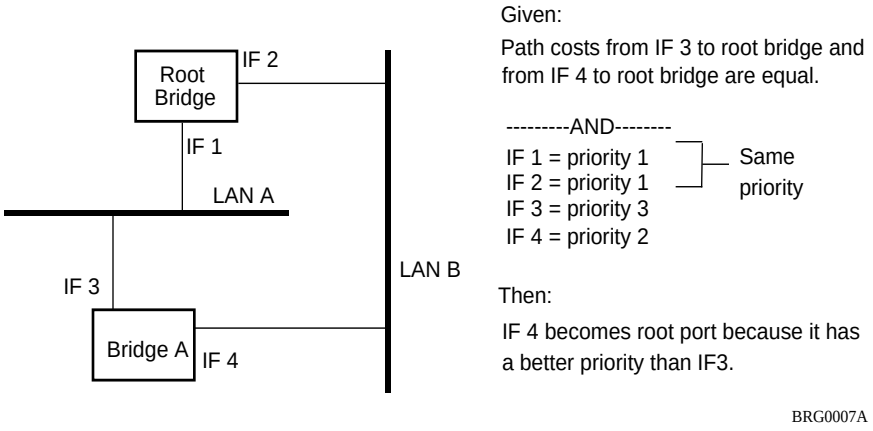


Figure 1-10. Root Port Determination (Equal Path Costs and Root Interface Priorities)

The spanning tree algorithm selects a bridge on each LAN as the designated bridge. The root port of this bridge has the lowest-cost path to the root bridge. All bridges turn off (set to blocking state) all of the lines except for the single line that is the shortest-cost path to the root and any line attached to the LANs for which the bridge serves as a designated bridge.

4. **Elect a designated port.**

   The spanning tree algorithm selects the port that connects the designated bridge to the LAN as the designated port. If there is more than one such port, the spanning tree algorithm selects the port with the lowest priority as the designated port. This port, which carries all extended network traffic to and from the LAN, is in the forwarding state.

Thus, the spanning tree algorithm removes all redundant ports (ports providing parallel connections) from service (places in the blocking state). If there is a topological change or a bridge or data-path failure, the algorithm derives a new spanning tree that may move some ports from the blocking to the forwarding state.

For example, in Figure 1-8, if all path costs are equal and Bridge 2 has the lowest-bridge priority (followed by Bridge 3, Bridge 4, and Bridge 1), the spanning tree algorithm may block Bridge 1/Interface 8 and Bridge 4/Interface 9 from service.

Figure 1-11 shows the resulting logical topology, which provides a loop-free topology with only a single path between any two hosts.

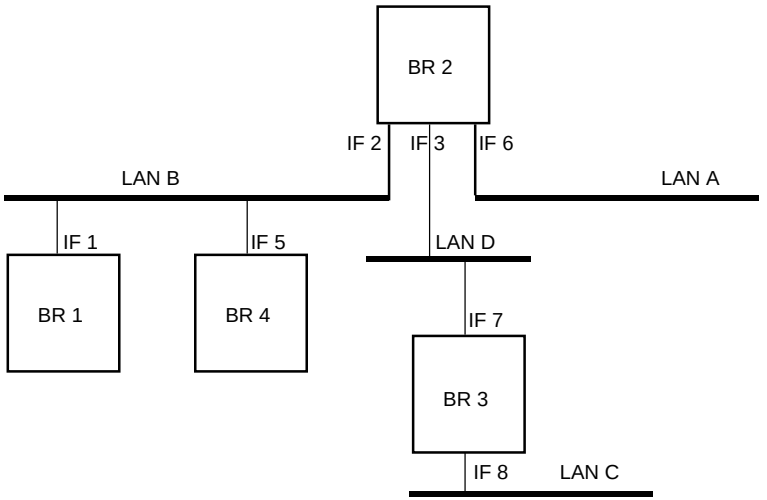
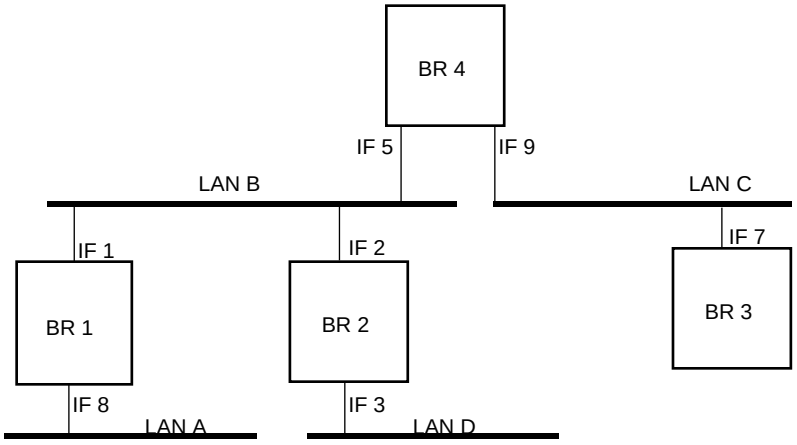


Figure 1-11. Spanning Tree (Loop-Free) Logical Topology

It is very important to configure the spanning tree parameters correctly. Consider the typical flow of traffic so that the logical topology that results from the spanning tree algorithm is appropriate for the network.

If, in the network shown in Figure 1-8, a majority of traffic originates on LAN A and is destined for LAN D, it is not practical to set the spanning tree parameters as shown in Figure 1-12. This figure illustrates an inefficient spanning tree topology for this network because the traffic from LAN A must traverse Bridge 1, LAN B, and Bridge 2 to get to LAN D. LAN B is then congested with unnecessary traffic.



Given:

All path costs are equal.
Interface (IF) number
denotes its priority.

----And---

BR 4 = priority 1
BR 3 = priority 2
BR 2 = priority 3
BR 1 = priority 4

Then:

Bridge 2/Interface 2 is blocked.
Bridge 3/Interface 7 is blocked.

Result:

Inefficient spanning
tree topology is created.

BRG009A

Figure 1-12. Inefficient Spanning Tree Topology

Filtering Frames

You use filters mainly for security reasons. They enable the bridge to relay or drop a particular frame based on user-selectable fields within each of the four encapsulation methods supported by the bridge. These encapsulation methods are

- Ethernet
- IEEE 802.2 LLC
- IEEE 802.2 LLC with SNAP header
- Novell proprietary

Refer to *Configuring Traffic Filters and Protocol Prioritization* for details about filters and how to configure them for the bridge.

Enabling Bridge Service

This section describes how to enable bridge service and, optionally, spanning tree on an interface. It assumes you have read *Configuring Routers* and that you have

1. **Opened a configuration file.**
2. **Specified router hardware if this is a local mode configuration file.**
3. **Selected the link or net module connector on which you are enabling bridge service, or configured a WAN circuit if this connector requires one.**

Enabling Bridge Service on an Interface

To enable bridge service without spanning tree, select Bridge from the Select Protocols menu and click on OK. The Select Protocols menu appears after you either select a link or net module connector, or finish configuring a WAN circuit.

When you enable bridge service without spanning tree, you need not specify any configuration information, because Configuration Manager supplies default values for the bridge parameters. The protocol pop-up window for the next enabled protocol appears, or, if only bridge is enabled on this circuit, the Bay Networks Configuration Manager window appears. To edit the default values for the bridge parameters, refer to Editing Bridge Parameters for instructions.

Enabling Spanning Tree on an Interface

To enable spanning tree on an interface, use the following procedure.

1. **From the Select Protocols menu, select the Spanning Tree option that is directly under the Bridge option.**

   Note that the Configuration Manager also selects the Bridge option because this Spanning Tree protocol cannot run without Bridge enabled.

2. **Click on OK.**

   The Spanning Tree Autoconfiguration window appears (Figure 1-13).

When you enable spanning tree service, you need only configure the Bridge Priority and Bridge MAC Address parameters. The Configuration Manager supplies default values for the remaining parameters. If you want to edit the default values, see "Editing Bridge Parameters" later in this section.

Note: Because the spanning tree is global (that is, it runs across all Bridge circuits), the Configuration Manager only displays the Spanning Tree Autoconfiguration window the *first* time you specify Spanning Tree for the Bridge. If you have previously specified Spanning Tree for source routing, this window will not appear. To change the parameter settings at a later time, refer to the "Editing Bridge Parameters" section.

3. **Configure the parameters, using the descriptions that follow as a guide.**
4. **When you have configured the required parameters, click on OK.**

   A pop-up window prompts

   ```
   Do you want to edit the Spanning Tree Interface Details?
   ```

5. **Click on Cancel to enable default Spanning Tree service and display the next protocol-specific pop-up window, or click on OK to edit the default spanning tree values.**

   (Refer to "Editing Bridge Parameters" for instructions.)

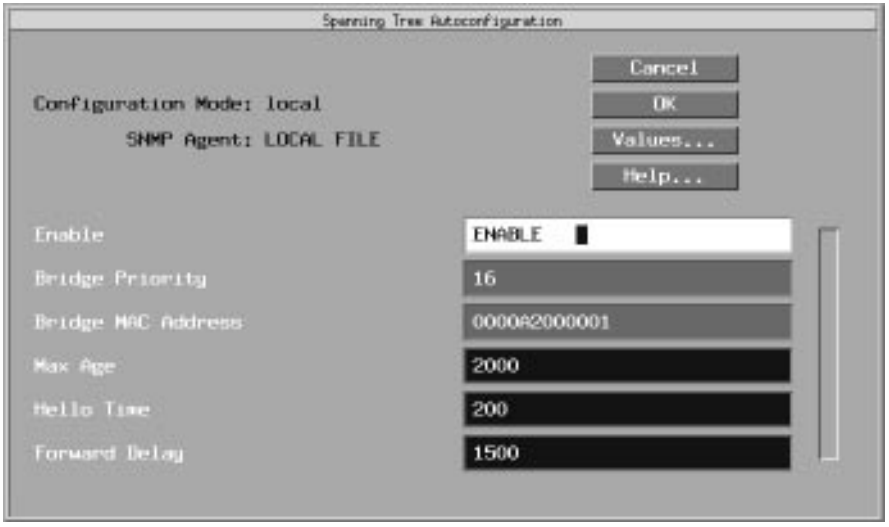


Figure 1-13. Spanning Tree Autoconfiguration Window

Parameter: **Bridge Priority**

Default: 128

Range: 0 to 65535

Function: Combined with the Bridge MAC Address parameter, assigns a 64-bit bridge ID to the router. This parameter supplies the most significant 16 bits of the bridge ID, while Bridge MAC Address supplies the remaining (least significant) 48 bits.

The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest bridge ID number. Thus, the lower the value you set for this parameter, the more likely it is that the router will be selected as the root bridge.

Instructions: Enter a decimal value from 0 to 65535.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.2.1.5

Parameter:	**Bridge MAC Address**
Default:	Defaults to a unique MAC address that the router automatically creates based on the router's backplane ID.
Options:	Any valid 48-bit MAC-level address
Function:	Combined with the Bridge Priority parameter, assigns a 64-bit bridge ID to the router. Bridge Priority supplies the most significant 16 bits of the bridge ID, while this parameter supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest bridge ID number. Thus, the lower the setting of Bridge Priority, the more likely it is that the router will be selected as the root bridge. In the event of equal Bridge Priority values, the value of this parameter determines the bridge's priority.
Instructions:	Enter a 48-bit MAC address expressed as a 12-digit hexadecimal value. We recommend that you set this parameter to the MAC address of one of the router's spanning tree ports, preferably the one with the lowest priority.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.5

Editing Bridge Parameters

Once you configure a circuit to support the bridge and, optionally, the spanning tree algorithm, you use Configuration Manager to edit the bridge and spanning tree parameters.

This section provides information on how to access and edit these parameters.

Note: If you enable the spanning tree algorithm for your network, the algorithm reconverges if you dynamically change any of the parameters described in the following sections.

You access all bridge parameters from the Configuration Manager window (Figure 1-14). (Refer to *Using Site Manager Software* guide for details on accessing this window.)

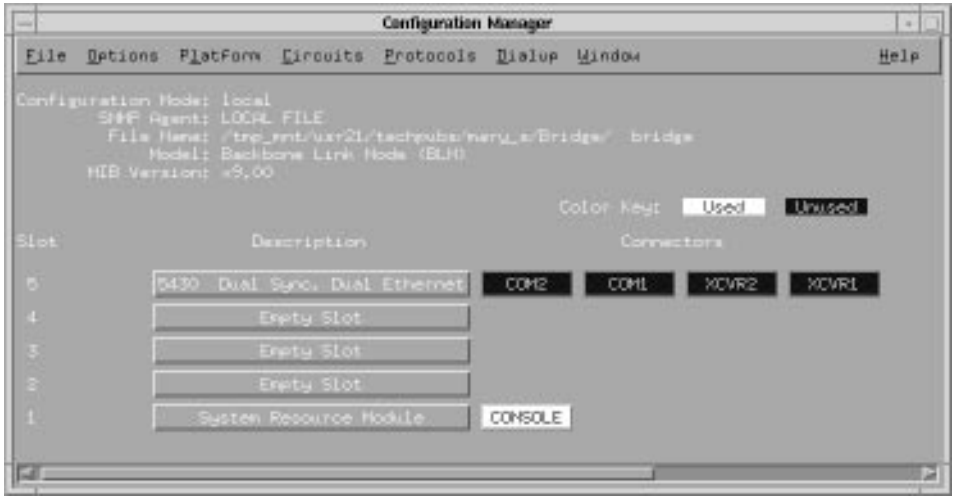


Figure 1-14. Configuration Manager Window

For each bridge and spanning tree parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Editing Bridge Global Parameters

To edit the bridge global parameters:

1. **Select Protocols > Bridge > Global from the Configuration Manager window (refer to Figure 1-14).**

   The Edit Bridge Global Parameters window appears (Figure 1-15).

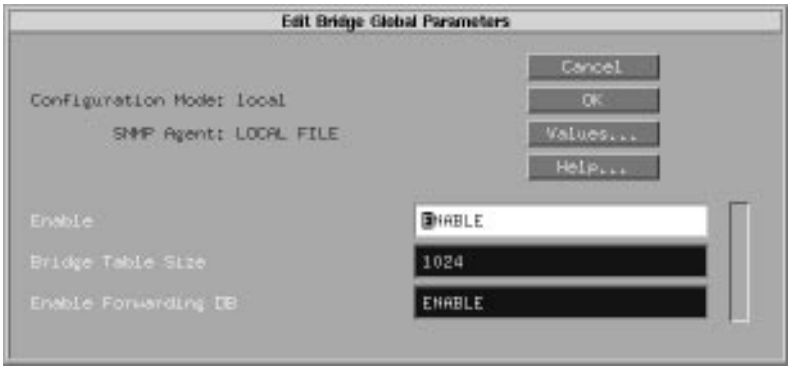


Figure 1-15. Edit Bridge Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

Bridge Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Bridge Global Parameters window (refer to Figure 1-15).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables bridging on the entire router.
Instructions:	Set to Disable if you want to disable bridging for all circuits on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.1.1.2

Parameter:	**Bridge Table Size**
Default:	1024 entries
Options:	1024 | 2048 | 4096 | 8192 | 16384 | 32768 | 65536 | 131072
Function:	Specifies the maximum number of MAC address entries allowed in the forwarding table. If you enter an invalid value, the system rounds up or down from the invalid value to the nearest valid value. If you increase the number of table entries, the bridge is more efficient but uses more memory. If you save a change to this parameter in dynamic mode, the bridge disables and then re-enables itself, thereby deleting all previously learned addresses.
Instructions:	Specify the table size, after accounting for the number of protocols running on your router and the size of the bridged network. The translation bridge, if configured, also adds addresses to this forwarding table. Therefore, if you configure the translation bridge, remember to account for the number of addresses it learns from the source route network. Select the 131072 option only if the router is running IP Host Only and no other protocols are running on the router. If you select 131072, the system automatically disables the next parameter, Enable Forwarding DB.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.1.1.5

Parameter:	**Enable Forwarding DB**
Default:	Enable
Options:	Enable | Disable
Function:	If you enable this parameter, the bridge maintains an additional table, equal in size to the forwarding table plus dynamically allocated memory for each MAC address. This additional table contains each MAC address in the forwarding table and the port from which the bridge learned the address. The table allows you to access MAC addresses and ports via the MIB. If you change the setting of this parameter in dynamic mode, the bridge disables and re-enables itself. If you change the setting to Disable, the bridge deletes all previously learned addresses, including those in the forwarding table.
Instructions:	Leave this parameter enabled if you want to view the MAC addresses in the forwarding table or the ports from which the bridge learned the addresses. Disable this parameter if you need to improve bridge performance.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.1.1.6

Editing Bridge Interface Parameters

To edit bridge interface parameters:

1. **Select Protocols > Bridge > Interfaces from the Configuration Manager window (refer to Figure 1-14).**

   The Bridge Interfaces window appears (Figure 1-16).

Figure 1-16. Bridge Interfaces Window

2. **Select the interface you want to edit.**
3. **Edit the parameters, using the descriptions in the next section as a guide.**
4. **Click on Apply to save your changes.**
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Bridge Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Bridge Interfaces window (refer to Figure 1-16).

Parameter:	**Enable**
Default:	If you added bridging using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable bridging on this circuit, the parameter defaults to Disable.
Options:	Enable | Disable
Function:	Toggles bridging on and off for this circuit only.
Instructions:	This parameter does not allow you to add bridging to this circuit. To add the bridging protocol to this circuit, you must use the Configuration Manager (see *Configuring Routers)*. Set this parameter to either Enable or Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.3.1.2

Parameter:	**Translational Bridge Enable**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether this transparent bridge interface participates in a transparent-to-source-routing translation-bridged network. Make sure you enable only one interface for translation bridging and that you disable this parameter for all other interfaces. Otherwise, translation bridging does not occur.
Instructions:	Set this parameter to Enable or Disable, depending on your interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.3.1.9

Editing Spanning Tree Global Parameters

To edit the spanning tree global parameters:

1. **Select Protocols > Bridge > Spanning Tree > Global from the Configuration Manager window (refer to Figure 1-14).**

   The Edit Spanning Tree Global Parameters window appears (Figure 1-17).

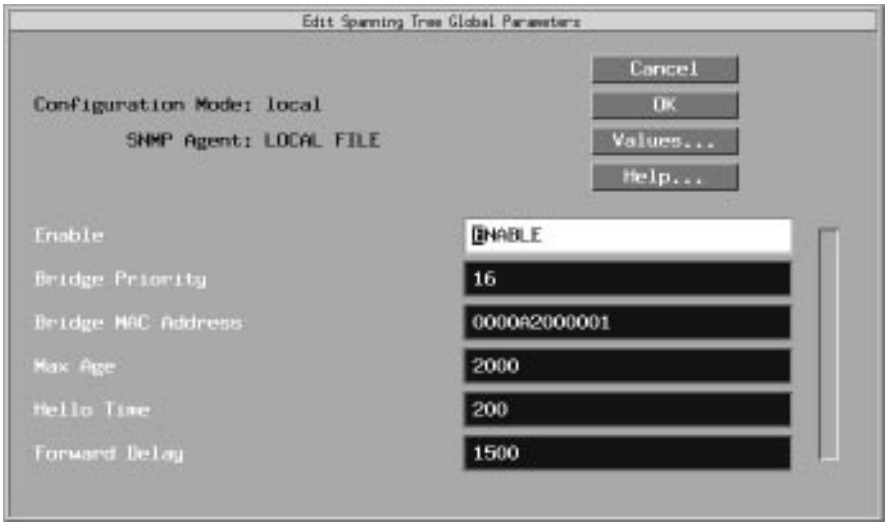


Figure 1-17. Edit Spanning Tree Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

Spanning Tree Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Spanning Tree Global Parameters window (refer to Figure 1-17).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables spanning tree on the entire router.
Instructions:	Set to Disable if you want to disable spanning tree for the entire router, or to Enable if you want to enable spanning tree for the entire router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.2

Parameter:	**Bridge Priority**
Default:	128
Range:	0 to 65535
Function:	Combined with the Bridge MAC Address parameter, assigns a 64-bit bridge ID to the router. This parameter supplies the most significant 16 bits of the bridge ID, while Bridge MAC Address supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest bridge ID number. Thus, the lower the value you set for this parameter, the more likely it is that the router will be selected as the root bridge.
Instructions:	Enter a decimal value from 0 to 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.5

Parameter:	**Bridge MAC Address**
Default:	Defaults to a unique MAC address that the router automatically creates based on the router's backplane ID.
Options:	Any valid 48-bit MAC-level address
Function:	Combined with the Bridge Priority parameter, assigns a 64-bit bridge ID to the router. Bridge Priority supplies the most significant 16 bits of the bridge ID, while this parameter supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest bridge ID number. Thus, the lower the setting of Bridge Priority, the more likely it is that the router will be selected as the root bridge. In the event of equal Bridge Priority values, the value of this parameter determines the bridge's priority.
Instructions:	Enter a 48-bit MAC address expressed as a 12-digit hexadecimal value. We recommend that you set this parameter to the MAC address of one of the router's spanning tree ports, preferably the one with the lowest priority.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.5

Caution: We recommend that you *not* change the following three spanning tree parameters (Max Age, Hello Time, and Forward Delay) unless absolutely necessary. However, if you do change them, you must follow these guidelines:

$$2 \times (\text{Forward Delay} - 1 \text{ Second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ Second})$$

BRG0010A

If the values for Max Age, Hello Time, and Forward Delay are not the same for each bridge in your network, the root bridge parameters rule the entire topology.

Parameter: **Max Age**

Default: 20 seconds (expressed in hundredths of a second: 2000)

Range: 6 to 40 seconds

Function: Specifies the maximum number of seconds that the router considers protocol information (BPDUs) valid. After this specified amount of time, the router times out and discards the information.

We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section.

Instructions: Either accept the default value or specify a new value. Make sure to express any new value in hundredths of a second.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.2.1.15

Parameter:	**Hello Time**
Default:	2 seconds (expressed in hundredths of a second: 200)
Range:	1 to 10 seconds
Function:	Specifies the interval in seconds between BPDUs transmitted by the bridge. BPDUs are periodic transmissions exchanged between bridges in the network to convey configuration and topology change data. We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section.
Instructions:	Either accept the default value or enter a new value. Make sure you enter the new value in hundredths of a second.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.16

Parameter:	**Forward Delay**
Default:	15 seconds (expressed in hundredths of a second: 1500)
Range:	4 to 30 seconds
Function:	Specifies the time in seconds that a circuit spends in the listening and learning states. If you set this parameter to the minimum value, the spanning tree converges at its fastest rate. As the spanning tree algorithm operates, it eventually places all circuits in either a forwarding (enabled) or blocking (disabled) state. In response to network topology changes, the spanning tree algorithm may change the state of specific circuits. To prevent network looping caused by sudden state changes, the spanning tree algorithm does not change circuits directly from the blocking to the forwarding state. Rather, it places them in two intermediate states: listening and learning. In the listening (standby) state, the circuit listens for network-generated BPDUs. It receives and drops all other traffic. When the forward delay timer expires, the spanning tree algorithm places the circuit in the learning state. In the learning state, the circuit receives both network-generated BPDUs and endstation-generated traffic that is subjected to the learning process but is not relayed. When the forward delay timer expires, the spanning tree algorithm places the circuit in the forwarding state. We recommend that you accept the default, 15 seconds; however, if you change the value, you must follow the guidelines listed previously in this section.
Instructions:	Either accept the default value or enter a new value. Make sure you enter the new value in hundredths of a second.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.1.17

Editing Spanning Tree Interface Parameters

To edit spanning tree interface parameters:

1. **Select Protocols > Bridge > Spanning Tree > Interfaces from the Configuration Manager window (refer to Figure 1-14).**

   The Spanning Tree Interfaces window appears (Figure 1-18).

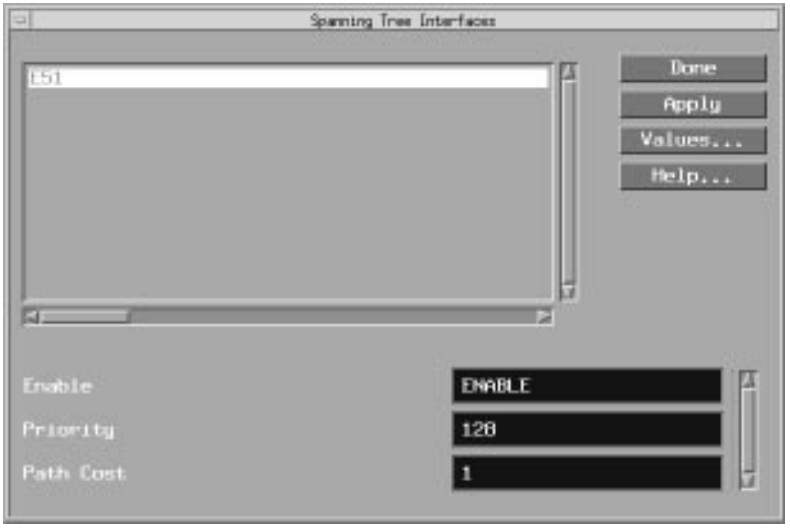


Figure 1-18. Spanning Tree Interfaces Window

2. **Select the interface you want to edit.**
3. **Edit the parameters, using the descriptions in the next section as a guide.**
4. **Click on Apply to save your changes.**
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Spanning Tree Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Spanning Tree Interfaces window (refer to Figure 1-18).

Parameter:	**Enable**
Default:	If you added spanning tree using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable.
Options:	Enable | Disable
Function:	Toggles spanning tree on and off for this circuit only.
Instructions:	This parameter does not allow you to add spanning tree to this circuit. To add the spanning tree to this circuit, you must use the Configuration Manager. (Refer to *Configuring Routers* for details.)
Instructions:	Set this parameter to Enable or Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.2.1.2

Parameter:	**Priority**
Default:	128
Range:	0 to 255
Function:	Assigns a priority to a bridge port. This interface priority value and the bridge ID (bridge priority + bridge MAC address) determine whether this port becomes the designated port when the spanning tree algorithm converges. The lower the priority value, the higher the priority, and the more likely it is that this port will be the designated port.
Instructions:	Either accept the default value or enter a new value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.2.1.4

Parameter:	**Path Cost**
Default:	1
Range:	1 to 65535
Function:	When this port is the root port, the path cost is the contribution of the path through this port to the total cost of the path to the root for this bridge. When this port is *not* the root port, the path cost is added to the designated cost for the root port and is used as the value of the root path cost offered in all configuration BPDUs transmitted by the bridge. To determine the path cost, use this formula: Interface Path Cost = 1000/Attached LAN speed in Mb/s
Instructions:	Enter a path cost value. For example, enter 100 if the attached LAN is Ethernet (1000/10 = 100).
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.2.2.1.7

Flushing the Forwarding Table

You can clear (flush) all MAC addresses from the bridge's forwarding table without bringing the bridge down and back up. This function is only available when you configure the bridge in dynamic mode.

To flush the tables, select Protocols > Bridge > Flush FWD Tables from the Configuration Manager window (refer to Figure 1-14). The system unlearns all MAC addresses it previously stored in its forwarding table and then displays a confirmation message.

Deleting the Bridge and Spanning Tree from the Router

To delete the bridge or spanning tree from all Bay Networks router circuits on which you enabled them, begin at the Configuration Manager window (refer to Figure 1-14):

1. **To delete the bridge and spanning tree, select Protocols > Bridge > Delete Bridge. To delete the spanning tree only, select Protocols > Bridge > Spanning Tree > Delete Spanning Tree.**

   A confirmation window appears asking whether you really want to delete the bridge or spanning tree.

2. **Click on OK.**

   Site Manager returns you to the Configuration Manager window.

   The bridge and/or spanning tree is no longer configured on the Bay Networks router.

Chapter 2
Using Source Routing Bridge Services

This chapter

- Contains an overview of source routing technology
- Describes how the Bay Networks source routing bridge works
- Includes a list of additional source routing reference material
- Lists implementation guidelines for adding source routing bridges to your network
- Describes how to enable source routing services on an interface
- Describes how to edit source routing parameters and delete source routing from the router

Source Routing Overview

Source routing networks consist of LAN segments connected by source routing bridges (Figure 2-1).

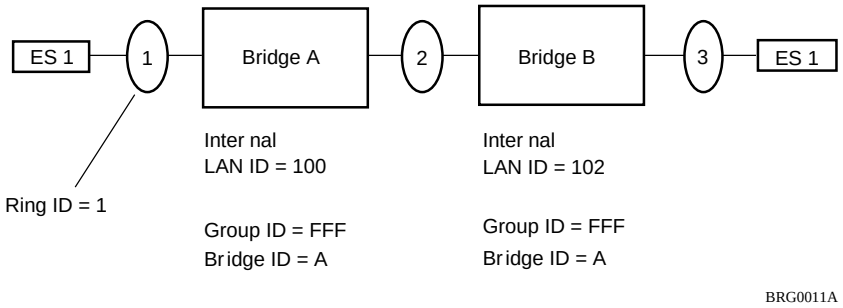


Figure 2-1. Source Routing Network

Each LAN segment has a unique network-wide identification number, or ring ID. Each source routing bridge also has an identification number, or bridge ID, and a unique network-wide internal or virtual LAN identification number, called an internal LAN ID.

For each Bay Networks source routing bridge in the network, you assign an additional routing identifier called a group LAN ID. The group LAN ID serves as a routing information field (RIF) placeholder and Bay Networks identifier.

How Source Routing Differs from Transparent Bridging

The Bay Networks source routing bridge differs from the Bay Networks transparent bridge (described in Chapter 1) in two ways:

- Source routing bridges can tolerate multiple paths between endstations in an extended network; transparent bridges require loop-free topologies.
- Source routing bridges require endstations to supply the bridging information needed to deliver a frame to a destination; transparent bridges use forwarding tables.

How Endstations on a Source Routing Network Discover Routes

The following sections describe the three processes that endstations on a source routing network use to learn the routes to destinations: all-paths broadcast routing, spanning tree broadcast routing, and specific routing.

All-Paths Broadcast Routing

An endstation that is configured for all-paths broadcast routing generates multiple frames that traverse all paths between source and destination endstations. These frames are *all-routes explorer* (ARE) or *all-paths explorer* (APE) frames.

When an endstation receives an ARE frame, a bridge within the source routing network appends a routing designator that identifies the incoming ring ID, internal LAN ID/bridge ID, and outgoing ring ID (Figure 2-2). For information on the spanning tree algorithm, refer to Chapter 1.

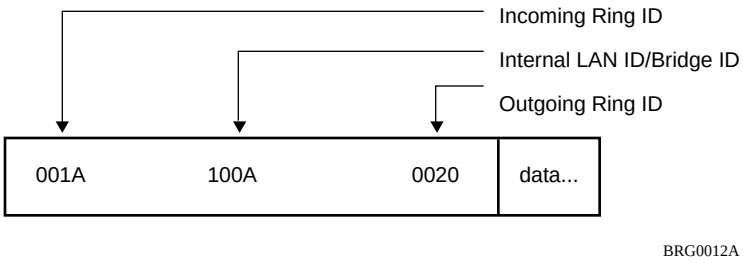


Figure 2-2. Source Routing Designator

After the bridge adds the routing designator, the other bridges send the frame out all ports (*floods* the frame). As a result, multiple copies of the same ARE frame can appear on a LAN, and the frame recipient can receive multiple copies of the frame (one copy for each possible path through the extended network).

Each ARE frame received by the destination endstation contains a unique sequenced list of routing designators tracing the frame's path through the source routing network.

Note: In a looped topology, the originating bridge may receive the ARE frame; the originating bridge discards the frame.

Spanning Tree Broadcast Routing

An endstation configured for spanning tree broadcast routing generates a single frame that follows a loop-free path from source to destination. This frame is a *spanning tree explorer* (STE).

When an endstation generates an STE frame, each bridge on the spanning tree forwards the frame onto all active (nonblocked) ports, except the port that received the frame. With spanning tree broadcast routing, one copy of the STE appears on each LAN and the frame recipient receives a single copy only.

Specific Routing

When an endstation receives an ARE or STE frame, it generates a single frame, called a *specifically routed frame* (SRF). The SRF traverses a specific path back to the source endstation; it contains a list of routing designators that maps a path through the extended network from source to destination.

When an endstation receives an SRF, each bridge between the source and destination examines the list of routing designators. The bridge forwards the SRF only if the bridge itself is on the specified path. Otherwise, it ignores the frame. When the SRF reaches the original source endstation, that station removes the routing information and stores it in its internal routing table.

Once the endstations discover a route and store the information in their routing tables, the endstations send specifically routed frames across the source routed network (Figure 2-3).

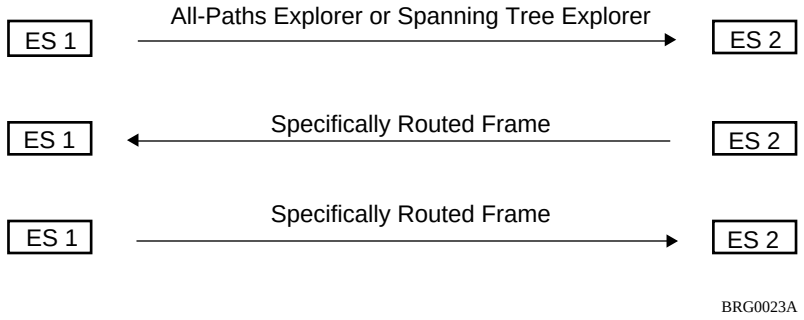


Figure 2-3. Route Discovery

Source Routing over IP Networks

The Bay Networks source routing bridge supports *Internet Protocol (IP) encapsulation*. IP encapsulation allows the source routing bridge to route frames to endstations located across an IP backbone network.

These frames use standard IP transmission services and a proprietary sequence maintenance protocol that ensures error-free, in-sequence delivery of IP encapsulated frames. The IP network can consist of any standard IP equipment and media.

How IP Encapsulation Works

When you enable IP encapsulation on a source routing bridge (thus making it an IP encapsulating bridge), you assign a *single* ring ID to the entire IP backbone network. The source routing bridge assigns only a single route descriptor to the frame's RIF to describe the entire internet, regardless of the IP network size that the frame traverses. Therefore, frames source routed over large IP networks can remain within maximum hop count restrictions.

Whenever a Bay Networks source routing bridge receives an explorer frame, the bridge sends it toward an IP encapsulating bridge, which resides at the edge of the IP backbone network. (For example, in Figure 2-4, Bridges A, B, and C are IP encapsulating bridges.) The IP encapsulating bridge encloses the source routed frame within an IP header before it sends the frame out onto the network. When the frame reaches a peer IP encapsulating bridge, the bridge removes the encapsulation from the frame and sends it out the appropriate source routing interfaces.

Each IP encapsulating bridge maintains a dynamic mapping of destination IP addresses to the ring and bridge IDs of their directly attached rings. When an IP encapsulating bridge receives a source routed frame, it performs these steps:

1. **Checks the frame's RIF for the ring and bridge ID that *immediately follow* the IP network ring and bridge ID in the RIF.**
2. **Looks up the IP address that corresponds with this ring and bridge ID.**
3. **Encapsulates the frame in an IP packet with the destination IP address.**
4. **Sends the frame out onto the IP network.**

For example, Figure 2-4 shows the IP mapping table for IP Encapsulating Bridge A.

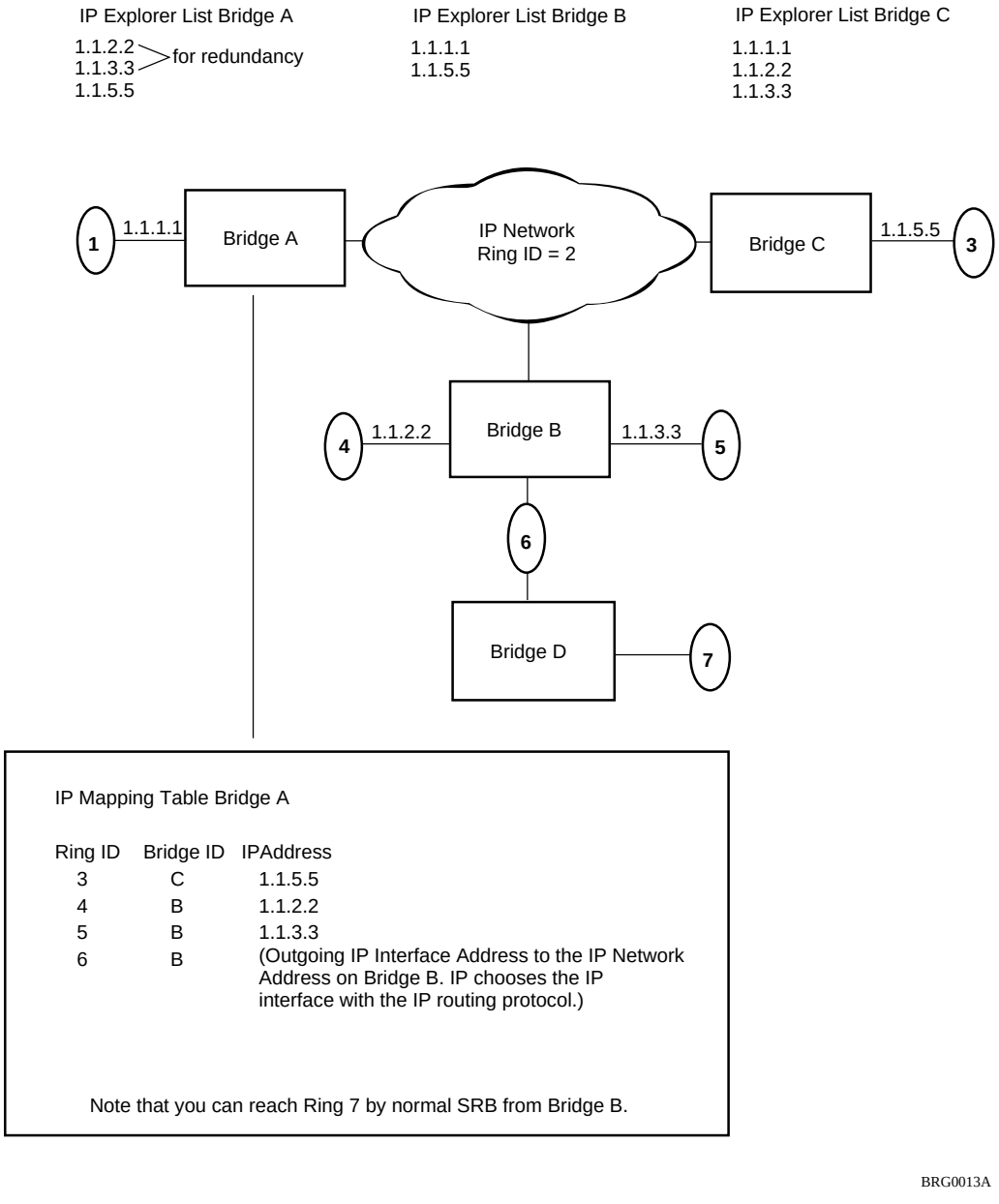


Figure 2-4. Source Routing over an IP Network

When Bridge A receives a source routed frame destined for an endstation on Ring 4, it examines the frame's RIF and locates the next ring ID (4) that immediately follows the IP network ring ID (2), as shown in Figure 2-5.

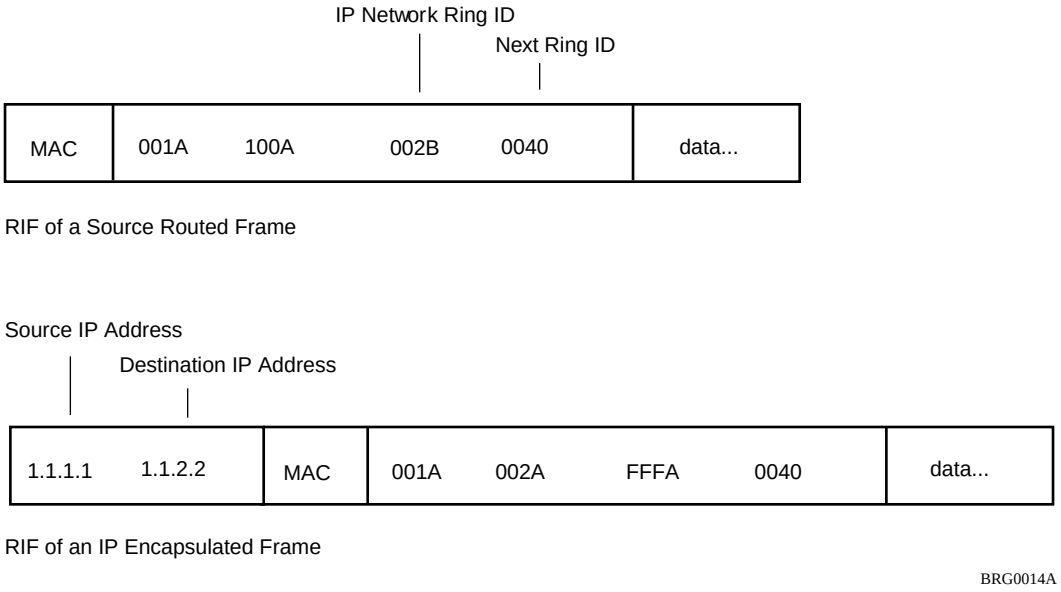


Figure 2-5. Examining the RIF Field of an SRF

Bridge A also examines the RIF to locate the bridge ID associated with the remote bridge used to reach Ring 4 (in this case, Bridge B). Then, Bridge A checks its mapping table for the IP address that corresponds to Ring ID 4 and Bridge B, and encapsulates the frame with an IP header. The IP header specifies its own source address, and the proper IP destination address (1.1.2.2). Finally, Bridge A forwards the packet onto the IP network.

You control which IP interfaces receive explorer frames by defining an *IP Explorer list* for each IP encapsulating bridge. For example, all of the IP encapsulating bridges that border the IP cloud in Figure 2-4 have IP explorer lists defined. Each bridge forwards explorer packets that are in its individual list toward the IP addresses. Note that the IP explorer lists for each bridge can vary. This allows you to control which IP networks receive explorer traffic.

IP Encapsulation Features

Bay Networks implementation of IP encapsulation allows you to:

- Configure redundant IP interfaces.

  You can configure redundant IP interfaces on the same router for critical network connections (for example, interfaces 1.1.2.2 and 1.1.3.3 on Bridge B). That way, if you disable one of the interfaces, the other interface can still accept IP traffic for the network. (When you enable redundant IP interfaces, you also increase explorer traffic on the network. Therefore, enable redundant interfaces selectively to reduce the impact on your network performance.)

- Expand your IP backbone network.

  You can expand your IP backbone to include any Bay Networks IP router on the network. You specify the router's IP address in the IP explorer list for each bridge.

  For example, Bridge A currently forwards all traffic destined for Ring 7 to IP interface 1.1.3.3. That router then forwards the traffic toward Ring 6 so that the router can source route it to Ring 7. If you add IP address 1.1.4.4. to the IP Explorer list for Bridge A, then Bridge A forwards all traffic destined for Ring 7 directly to IP interface 1.1.4.4. By expanding your IP backbone, the source routing bridge can route through more stations, but it still can only add a single hop to a packet's RIF.

- Reduce excess broadcast traffic on your IP network.

  You can reduce the number of broadcast and explorer packets that traverse the network by constructing *directed explorer filters. (*Refer to *Configuring Traffic Filters and Protocol Prioritization* for information on how to create filters that forward IP explorer frames to specific addresses.)

- Configure both IP encapsulation support and source route endstation support on the same interface.

  IP encapsulation support works independently of source route endstation support. However, you can enable both on the same circuit.

Source Route Endstation Support

The Bay Networks routers running IP, IPX, XNS, AppleTalk, and VINES protocols support support routing over Token Ring networks that contain one or more source routing bridges. This feature is called *source route endstation support*.

In a source routing network, every endstation that sends out a frame supplies the frame with the necessary route descriptors so that the router can source route it across the network. Thus, for routers to route packets across a source routing network, *they must act like endstations*; the routers must supply route descriptors for each packet before they send it out onto the network.

When you enable end-node support and a Bay Networks router running IP, IPX, XNS, AppleTalk, or VINES receives a packet and determines that the packet's next hop is across a source routing network, the router performs these steps:

1. **Adds the necessary RIF information to the packet's MAC header**
2. **Sends the packet out onto the network where it is source routed toward the next hop**

When the peer router receives the packet from the Token Ring network, it strips off the RIF field and continues to route the packet toward the destination network address (refer to Figure 2-6).

You configure source route end-node support for each individual routing protocol on a per-circuit basis.

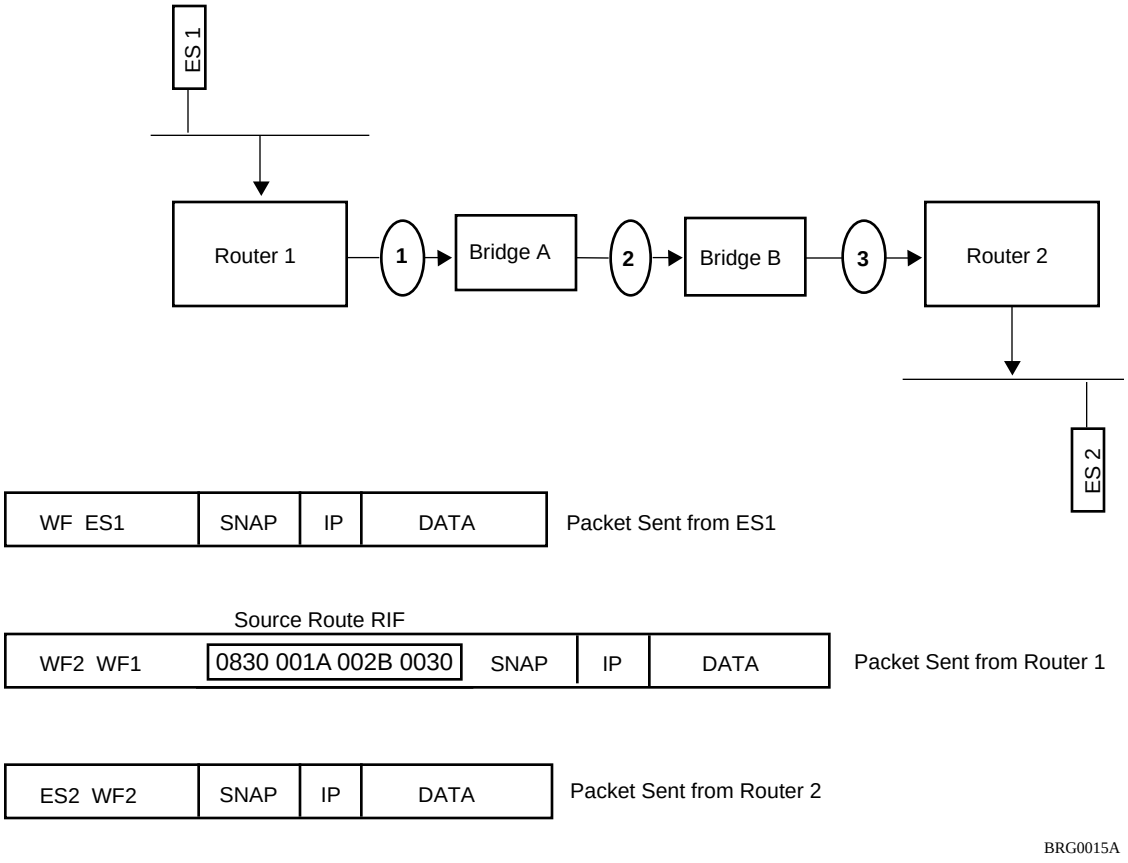


Figure 2-6. IP Routers Source Routing across a Token Ring Network

How the Bay Networks Source Routing Bridge Works

This section shows examples of how the Bay Networks source routing bridge routes frames through a Token Ring network. It also describes how the source routing bridge routes frames across an IP backbone network (called *IP encapsulation*).

Source Routing across a Token Ring Network

The Bay Networks source routing bridge handles incoming packets differently, depending on the source routing bridge's position in the Token Ring network. To demonstrate, the following sections describe the routing information field (RIF) of a frame as it moves back and forth between Endstation 1 (ES1) and Endstation 2 (ES2) (Figure 2-7).

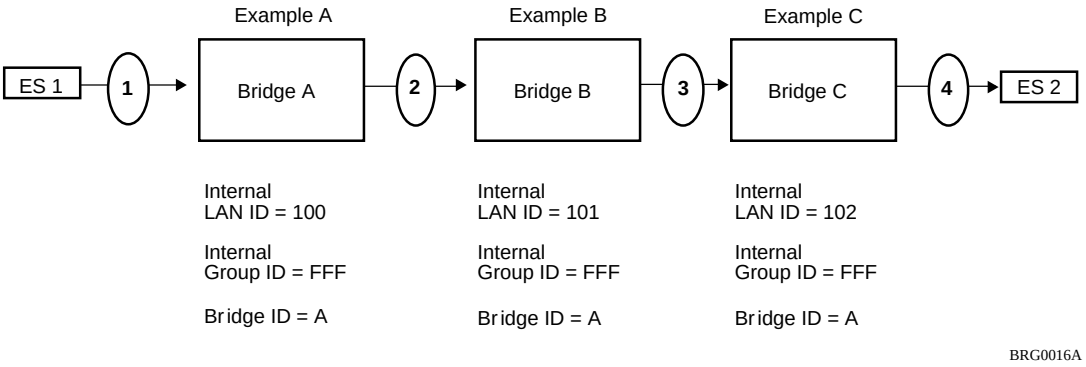


Figure 2-7. Tracking an Explorer Frame

First, we track the RIF of an explorer frame sent from ES1 to ES2. Then, we track the RIF of a specifically routed frame sent back from ES2 to ES1.

The size of the RIF is variable. It contains the routing information required to transmit the frame across the network.

Although the following examples show only the Bay Networks source routing bridge, other IBM-compatible source routing bridges can reside in the same network.

How the Source Routing Bridge Handles Explorer Frames

This section provides instructions on how the Bay Networks source routing bridge handles explorer frames (AREs or STEs) sent from ES1 to ES2 (refer to refer to Figure 2-7). Each bridge's internal LAN ID, group LAN ID, and bridge ID is in hexadecimal format below the bridge.

- Example A describes the actions of the first Bay Networks bridge.
- Examples B and C describe the actions of other Bay Networks bridges in the explorer frame's path.

Example A: First bridge to receive the explorer frame

The frame received by Bridge A from Ring 1 did not traverse any other bridges. This bridge adds the following information in the RIF before it transmits the frame toward Ring 2 (refer to Figure 2-8):

- Incoming ring ID/bridge ID
- Internal LAN ID/bridge ID
- Outgoing ring ID/bridge ID 0

Examples B and C: Other bridges that receive the explorer frame

The explorer frame received by Bridges B and C contains internal LAN IDs and bridge numbers, indicating that this frame traversed at least one other Bay Networks bridge. These bridges perform the following steps in the RIF before transmitting the frame toward Rings 3 and 4 (refer to Figure 2-8):

1. **Remove the last internal LAN ID**
2. **Replace the incoming ring ID and bridge ID 0 with its own bridge ID**
3. **Add its own internal LAN ID/bridge ID**
4. **Add the outgoing ring ID/bridge ID 0**

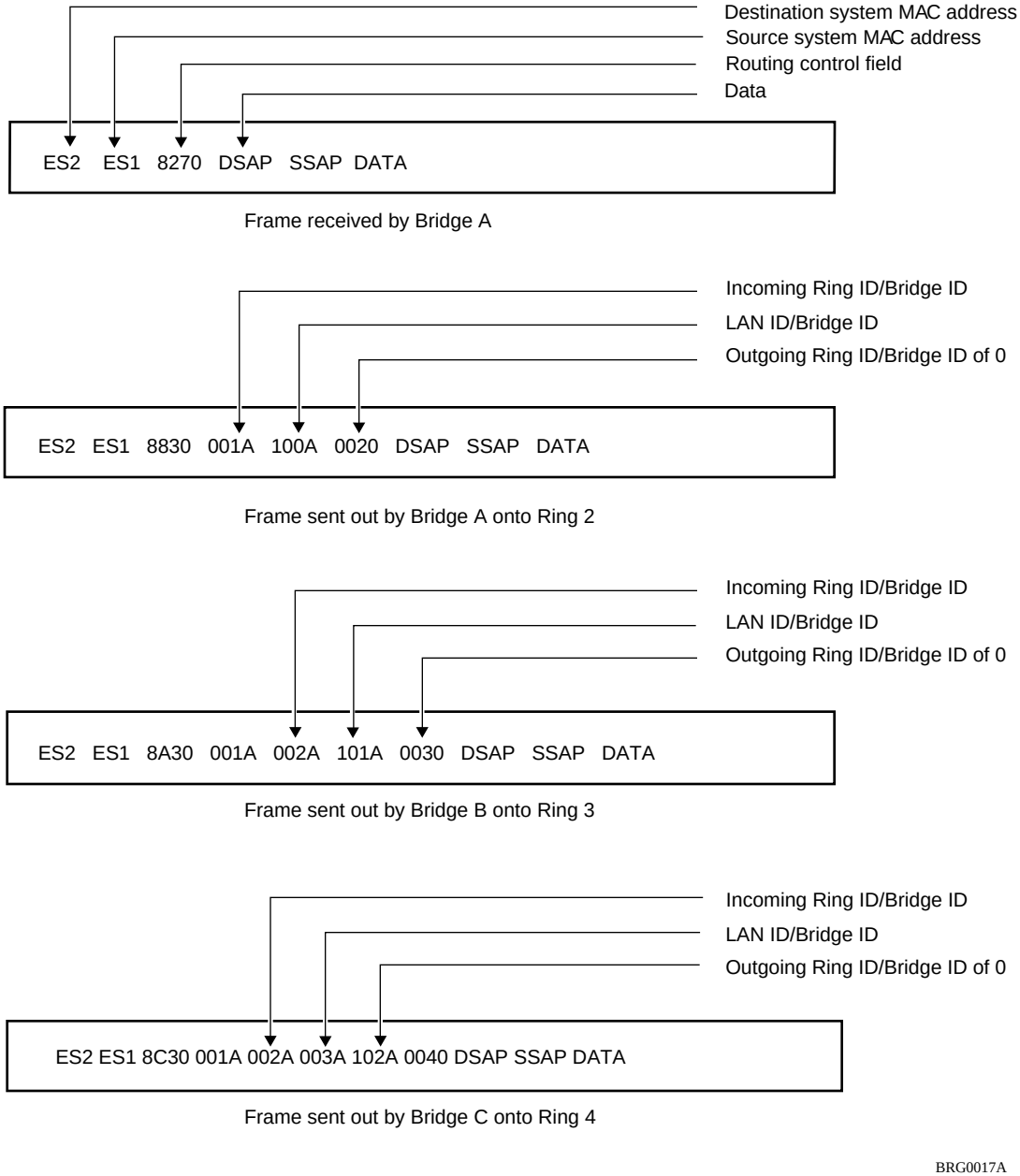

Destination system MAC address
Source system MAC address
Routing control field
Data
ES2 ES1 8270 DSAP SSAP DATA
Frame received by Bridge A
Incoming Ring ID/Bridge ID
LAN ID/Bridge ID
Outgoing Ring ID/Bridge ID of 0
ES2 ES1 8830 001A 100A 0020 DSAP SSAP DATA
Frame sent out by Bridge A onto Ring 2
Incoming Ring ID/Bridge ID
LAN ID/Bridge ID
Outgoing Ring ID/Bridge ID of 0
ES2 ES1 8A30 001A 002A 101A 0030 DSAP SSAP DATA
Frame sent out by Bridge B onto Ring 3
Incoming Ring ID/Bridge ID
LAN ID/Bridge ID
Outgoing Ring ID/Bridge ID of 0
ES2 ES1 8C30 001A 002A 003A 102A 0040 DSAP SSAP DATA
Frame sent out by Bridge C onto Ring 4
BRG0017A

Figure 2-8. Structure of an Explorer Frame

How the Source Routing Bridge Handles Specifically Routed Frames

This section describes how the Bay Networks source routing bridge handles specifically routed frames (SRFs) sent from ES2 to ES1. Depending on the bridge's position in the network, the bridge handles the SRFs differently (Figure 2-9).

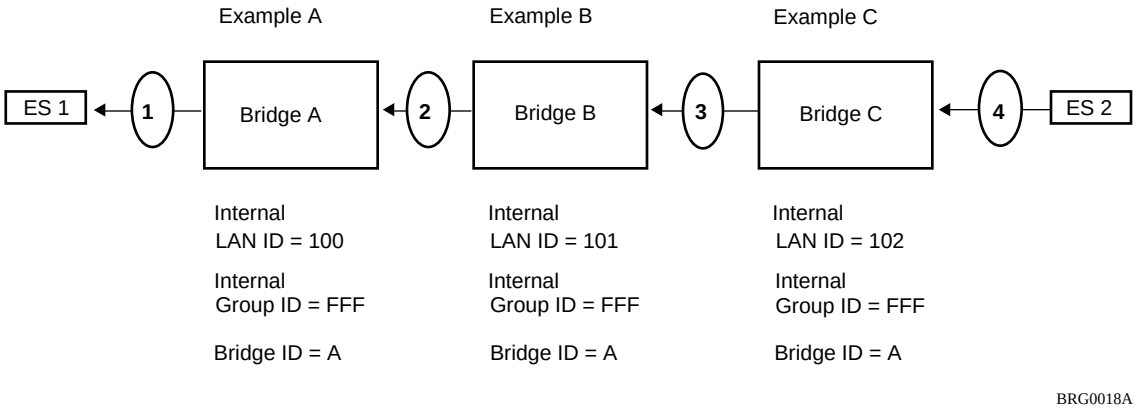


Figure 2-9. Tracking a Specifically Routed Frame from ES2 to ES1

If there is only a single bridge ID in the RIF, then the Bay Networks bridge transmits the frame to the outgoing circuit without modification. This is true only when the frame traverses a single Bay Networks bridge (or any combination of third-party bridges) between the source and destination endstation.

If there are multiple bridge IDs in the RIF, then:

- Example A describes the actions of a Bay Networks bridge if it is the first bridge to handle the SRF.
- Example B describes the actions of a Bay Networks bridge if there are multiple bridge IDs in the RIF, and the bridge is between the first and last Bay Networks bridge to handle the SRF.
- Example C describes the actions of a Bay Networks bridge if there are multiple bridge IDs in the RIF, and the bridge is the last Bay Networks bridge to handle the SRF.

Example A: First of several bridges to receive the SRF

The frame received by Bridge C from Ring 4 did not traverse any other Bay Networks bridges (but there are multiple bridge IDs in the RIF, so it will eventually). This bridge performs the following steps in the RIF before it transmits the frame toward Ring 3 (refer to Figure 2-10):

1. **Changes the destination system's MAC address at the beginning of the frame to a Bay Networks group address.**

   This address is C000A2FFFFFF*x*, where *x* is the bridge ID of the next Bay Networks bridge specified by the RIF.

2. **Removes its own internal LAN ID and inserts the group LAN ID before the last incoming ring and bridge ID listed in the RIF (refer to Figure 2-10).**

   Eventually, the internal LAN ID of the last Bay Networks bridge along the frame's path replaces the group LAN ID.

3. **Copies the destination system's MAC address into the data portion of the frame.**

Example B: Between the first and last bridges to receive the SRF

The frame received by Bridge B from Ring 3 traversed at least one other Bay Networks bridge. However, this is not the last Bay Networks bridge that the frame must traverse. This bridge performs the following steps in the RIF before transmitting the frame toward Ring 2 (Figure 2-10):

1. **Locates the bridge ID, which is at the end of the group address.**
2. **Changes the bridge ID at the end of the group address to the bridge ID of the next Bay Networks bridge in the RIF. (Only if it differs from the value already in place. In this example, all bridge IDs are the same, so the frame is not modified.)**

Example C: Last of several bridges to receive the SRF

The frame received by Bridge A is the last of several Bay Networks bridges traversed by the frame. This bridge performs the following steps in the RIF before it transmits the frame toward Ring 1 (refer to Figure 2-10):

1. **Replaces the Bay Networks group address with the destination MAC address that was saved to the data field**
2. **Replaces the group LAN ID with its own internal LAN ID**

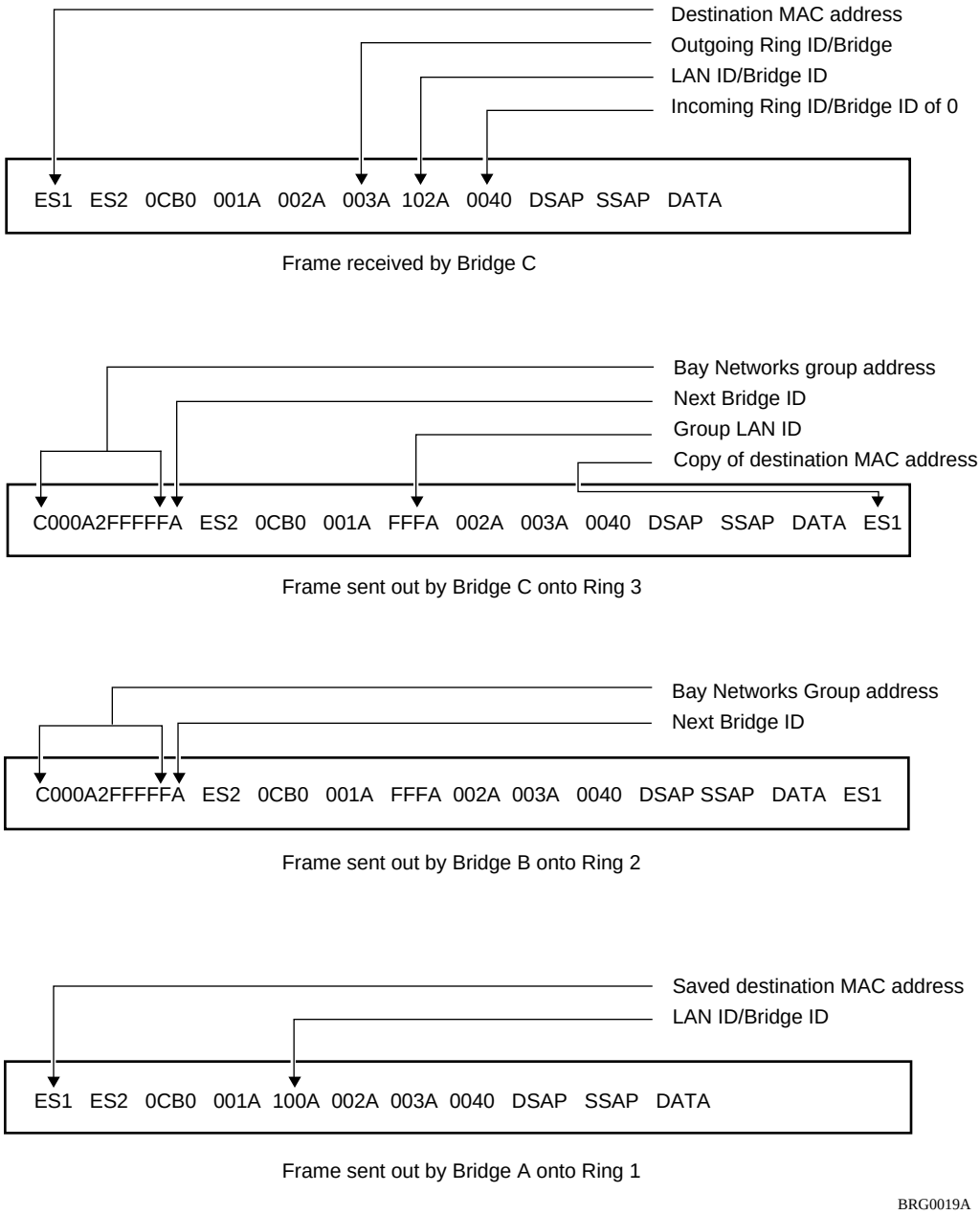

Destination MAC address
Outgoing Ring ID/Bridge
LAN ID/Bridge ID
Incoming Ring ID/Bridge ID of 0
ES1 ES2 0CB0 001A 002A 003A 102A 0040 DSAP SSAP DATA
Frame received by Bridge C
Bay Networks group address
Next Bridge ID
Group LAN ID
Copy of destination MAC address
C000A2FFFFFA ES2 0CB0 001A FFFA 002A 003A 0040 DSAP SSAP DATA ES1
Frame sent out by Bridge C onto Ring 3
Bay Networks Group address
Next Bridge ID
C000A2FFFFFA ES2 0CB0 001A FFFA 002A 003A 0040 DSAP SSAP DATA ES1
Frame sent out by Bridge B onto Ring 2
Saved destination MAC address
LAN ID/Bridge ID
ES1 ES2 0CB0 001A 100A 002A 003A 0040 DSAP SSAP DATA
Frame sent out by Bridge A onto Ring 1
BRG0019A

Figure 2-10. Structure of a Specifically Routed Frame from ES2 to ES1

Source Routing across an IP Network

This section provides details on how IP encapsulation works by tracing a specifically routed frame as it is sent out from Endstation 1, traverses several bridges and an IP network, and finally arrives at Endstation 2 (Figure 2-11).

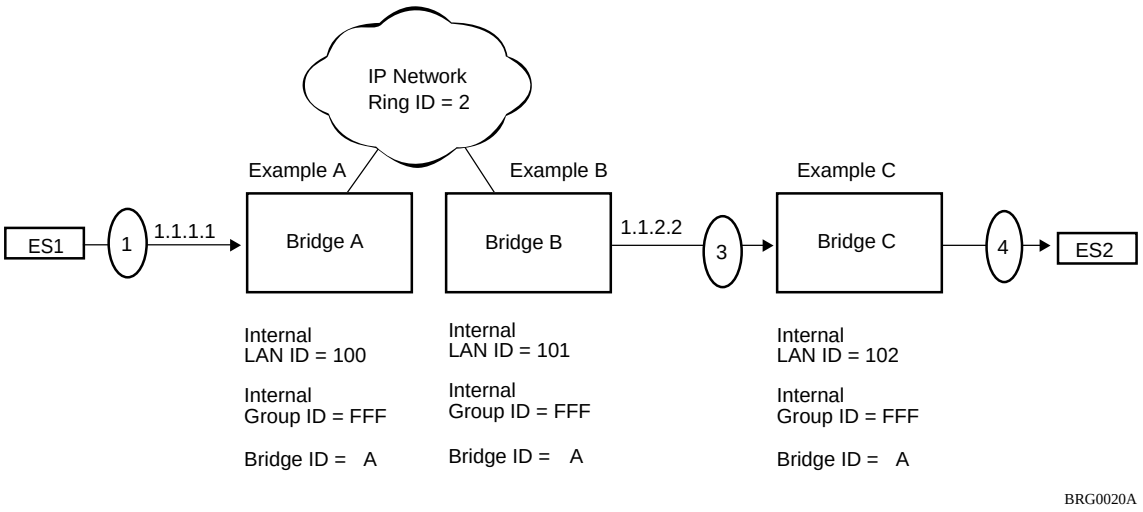


Figure 2-11. Tracking an IP-Encapsulated Frame from ES1 to ES2

Note: At this point, assume that explorer packets have traversed the network and identified the paths to all reachable interfaces.

To demonstrate IP encapsulation, this section traces a specifically routed frame as it is sent out from Endstation 1 and arrives at Endstation 2:

- Example A describes the actions of the first Bay Networks bridge to handle the SRF. This bridge encapsulates the frame with an IP header before it sends the frame out onto the IP network.
- Example B describes the actions of a Bay Networks bridge that is in between the first and last Bay Networks bridges to handle the SRF. This bridge removes the IP header from the frame before it source routes the frame to the next bridge.
- Example C describes the actions of the last bridge of several Bay Networks bridges to handle the SRF.

Example A: First of several bridges to receive the SRF

Bay Networks Bridge A is the first to receive the frame from Ring 1. Bridge A performs the following steps in the RIF before it transmits the frame onto the IP network (refer to Figure 2-12):

1. **Removes its own internal LAN ID.**
2. **Inserts the group LAN ID before the last incoming ring and bridge ID listed in the RIF (refer to Figure 2-12).**

   Eventually, the internal LAN ID of the last Bay Networks bridge along the frame's path replaces the group LAN ID.
3. **Adds an IP header containing the destination address 1.1.2.2 onto the frame and sends it toward the IP network.**

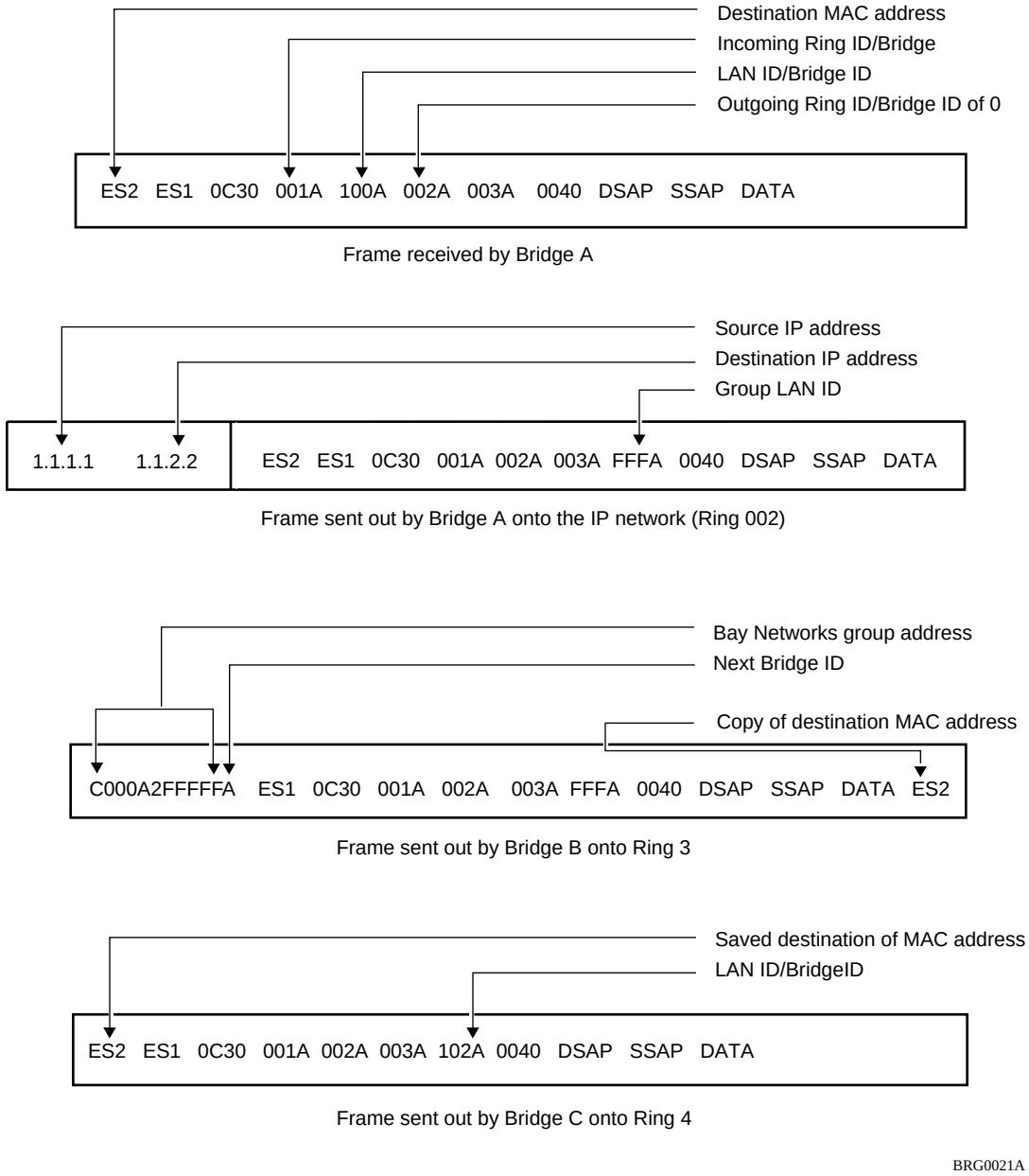

Destination MAC address
Incoming Ring ID/Bridge
LAN ID/Bridge ID
Outgoing Ring ID/Bridge ID of 0
ES2 ES1 0C30 001A 100A 002A 003A 0040 DSAP SSAP DATA
Frame received by Bridge A
Source IP address
Destination IP address
Group LAN ID
1.1.1.1 1.1.2.2 ES2 ES1 0C30 001A 002A 003A FFFA 0040 DSAP SSAP DATA
Frame sent out by Bridge A onto the IP network (Ring 002)
Bay Networks group address
Next Bridge ID
Copy of destination MAC address
C000A2FFFFFA ES1 0C30 001A 002A 003A FFFA 0040 DSAP SSAP DATA ES2
Frame sent out by Bridge B onto Ring 3
Saved destination of MAC address
LAN ID/BridgeID
ES2 ES1 0C30 001A 002A 003A 102A 0040 DSAP SSAP DATA
Frame sent out by Bridge C onto Ring 4
BRG0021A

Figure 2-12. Structure of an IP-Encapsulated Frame from ES1 to ES2

Example B: Between the first and last bridges to receive the SRF

Bay Networks Bridge B receives the frame from the IP network (Ring 2) and performs the following steps on the RIF before it transmits the frame toward Ring 3 (refer to refer to Figure 2-12):

1. **Strips the IP header from the packet.**
2. **Changes the destination system's MAC address at the beginning of the frame to a Bay Networks group address.**

   This address appears as C000A2FFFFFF*x*, where *x* is the bridge ID of the next Bay Networks bridge specified by the RIF.
3. **Copies the destination system's MAC address into the data portion of the frame.**
4. **Locates the bridge ID, which is at the end of the group address, and sends it to the bridge ID of the next Bay Networks bridge in the RIF.**

Example C: Last of several bridges to receive the SRF

The last Bay Networks bridge to receive the frame performs the following steps in the RIF before it transmits the frame toward Ring 4 (refer to refer to Figure 2-12):

1. **Replaces the Bay Networks group address with the destination MAC address that was saved to the data field.**
2. **Changes the group LAN ID to its own internal LAN ID.**

IP Encapsulation Guidelines

When using IP encapsulation, the following guidelines apply:

- Do not configure source routing on WAN links connecting the remote routers.
- Define IP addresses in the IP explorer list so that the source routing bridge can send AREs to those addresses.
- Configure IP on the port. The IP address automatically resides in the routing table.
- Define at least two IP address for each router in another router's ARE explorer table. If the service provided by one token ring interface is disabled, the router can still forward AREs.
- Alternatively, you could configure a connectionless IP address on each router and configure only the connectionless address. This would reduce explorer traffic but would ensure that the IP address is up.

Note: Each IP address on a router that receives an ARE forwards the ARE through all other source routed interfaces. This can cause duplicate AREs on the network, but it ensures redundancy if the service of any token ring interface is interrupted.

Source Routing over Frame Relay Networks

The Bay Networks source routing bridge supports source routing over Frame Relay networks, using RFC 1490 standard Frame Relay encapsulation and Bay Networks proprietary Frame Relay encapsulation.

To select proprietary or RFC 1490 standard Frame Relay encapsulation, use the Encapsulation Format parameter as described in the section "Source Routing Interface Parameter Descriptions" later in this chapter.

Source Routing over FDDI

The Bay Networks source routing bridge supports communications between Token Ring endstations and FDDI endstations, using standard native encapsulation and proprietary encapsulation. Use Bay Networks proprietary encapsulation if you want to communicate with a Version 7 router running source routing over FDDI.

To select proprietary or standard encapsulation, use the Encapsulation Format parameter as described in the section "Source Routing Interface Parameter Descriptions" later in this chapter.

For More Information about Source Routing

The following documents provide technical details on Source Routing Protocol implementation:

IBM Token Ring Network Architecture Reference. Third Edition (SC3D-3374-D2*)*. New York: IBM Corporation, September, 1989.

Source Routing Appendix to IEEE Standard 802.1d. Media Access Control (MAC) Bridges. Project 802.5m - Draft 71991.

Perlman, Radia. *Interconnections: Bridges and Routers*. Reading, Massachusetts: Addison-Wesley Publishing Company, First printing, May, 1992.

Implementation Notes

This section contains some basic guidelines for adding Bay Networks source routing bridges to your network. It also describes some of the configuration features that may match your network requirements.

Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs

When you enable the source routing bridge on the router, you must specify its bridge ID and internal LAN ID. The source routing bridge uses these routing designators and the group LAN ID to source-route packets through the network. The following sections describe each of these routing designators in detail.

Bridge ID

The bridge ID is a standard source routing designator that identifies a bridge in the network. When you assign the bridge ID, make sure you follow these guidelines:

- Assign the same bridge ID to all other Bay Networks source routing bridges on the network unless the bridges operate in parallel.
- Assign bridge IDs to Bay Networks bridges that are *unique* among all bridges on the network.

- Assign to third-party routers bridge IDs that differ from Bay Networks source routing bridge IDs.

If two or more Bay Networks bridges operate in parallel, you must assign different bridge IDs. You must also specify the other Bay Networks bridge ID in the entry list for each bridge.

For example, in Figure 2-13, Bay Networks Bridges A, C, and D all have the same bridge ID (A). However, because Bridges B and C operate in parallel, Bridge B has a different bridge ID (B). You specify this bridge ID (B) in the Bridge Entry list for Bridges A, C, and D. This ensures that the bridges know Bridge B is active on the network. Similarly, you specify the bridge ID (A) for Bridge B on the Bridge Entry list so that it knows Bridges A, C, and D are active on the network.

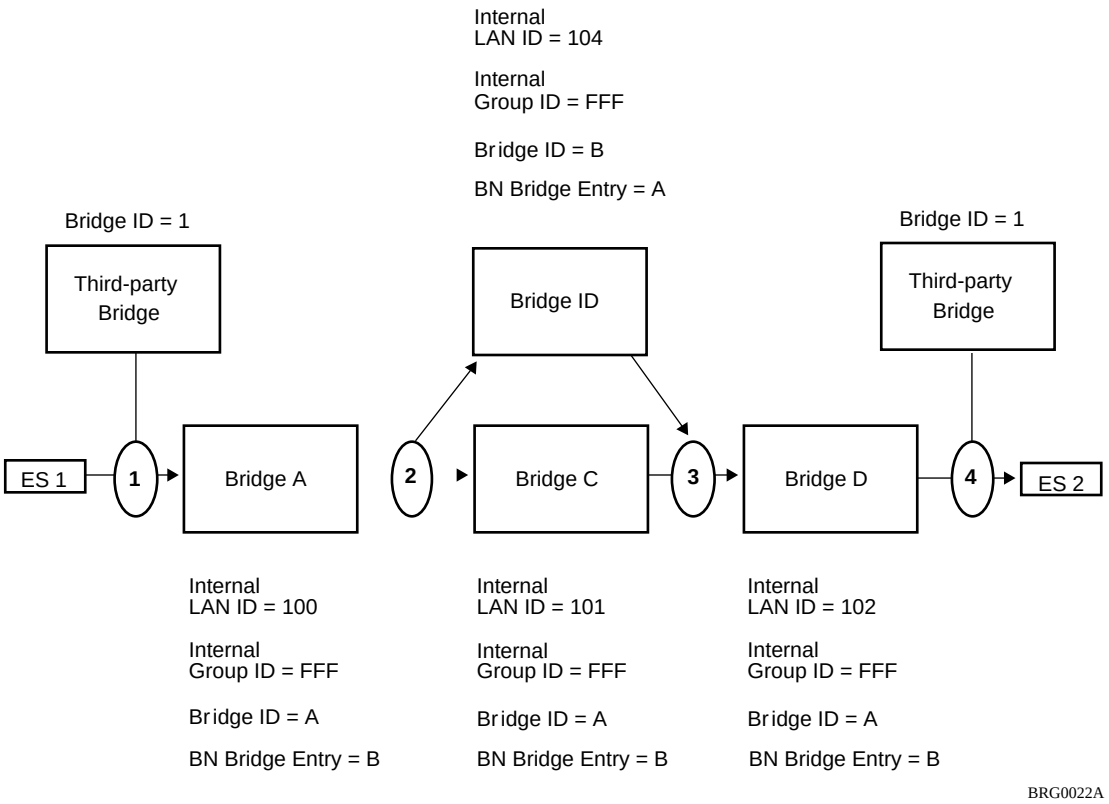


Figure 2-13. Parallel Operation

Internal LAN ID

The internal LAN ID is a source routing designator that identifies the virtual LAN on which frames travel. When you configure the Bay Networks source routing bridge, you must assign a globally unique internal LAN ID to each bridge on which you enabled source routing. For example, in Figure 2-13, Source Routing Bridges A, B, C, and D all have unique internal LAN IDs.

Group LAN ID

The group LAN ID is a Bay Networks proprietary routing designator that helps the source routing bridges in your network identify the last Bay Networks bridge in their path. When you configure the Bay Networks source routing bridge, make sure you follow these configuration guidelines:

- Assign the *same* group LAN ID to all source routing bridges in the network.
- Assign a group LAN ID to all bridges in your network. This number must be *different* from the LAN ID value assigned to any other bridges in the network.

Configuring IP Encapsulation Support

IP encapsulation support allows you to source route frames between Bay Networks bridges over IP networks. When you enable IP encapsulation on the source routing bridge, make sure you follow these guidelines:

- Enable at least one IP interface on those routers through which you want to source route packets. You can enable IP on any circuit on any slot on the router; it does not have to be the same circuit on which you enabled source routing. (Refer to *Configuring IP Services* for details on enabling IP on a circuit.)
- Configure redundant IP interfaces on different slots on the same router if you want the router to receive broadcasts for backup purposes.

  Alternatively, you could configure a connectionless IP address on each router and configure only the connectionless address. This results in reduced explorer traffic but ensures that the IP interface is always available.
- Enable source routing on the circuits of those bridges through which you want to source route frames. (Refer to "Enabling Source Routing Services" for details on enabling source routing on a circuit.)

- Specify a ring ID for the backbone IP network to which the source routing interface connects. You enter the IP network's ring ID using the Conn. IP NTWK Ring Number parameter for each source routing bridge. (Refer to "Editing Source Routing Global Parameters" later in this chapter for details on accessing this parameter.) Specify the same IP network ring ID for each Bay Networks source routing bridge that connects to the network.
- Enable IP encapsulation on the source routing bridges that connect to the IP backbone. You reset the IP Encapsulation parameter to Enable for each source routing bridge. (Refer to "Editing Source Routing Global Parameters" later in this chapter for details on accessing this parameter.)
- Specify the IP Explorer list for each source routing interface that connects to the IP backbone.

  The IP Explorer list defines the IP addresses that will receive explorer frames from the bridge. These IP addresses are assigned to the token rings of remote users. (Refer to "Adding or Deleting an IP Address on the IP Explorer Address List" later in this chapter for details on the IP Explorer list.)
- Create directed explorer filters to reduce excess broadcast traffic on the network. (Refer to *Configuring Traffic Filters and Protocol Prioritization* for details on filters.)

Enabling Source Routing Services

This section describes how to enable the following services on an interface:

- Source routing
- Source routing spanning tree

It assumes you have read *Configuring Routers* and that you have

1. **Opened a configuration file**
2. **Specified router hardware if this is a local mode configuration file**
3. **Selected the link or net module connector on which you are enabling source routing, or configured a WAN circuit if this connector requires one**

When you enable any of the source routing services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters. If you want to edit these default values, refer to "Enabling Source Routing Services on an Interface"

For each source routing parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Enabling Source Routing Services on an Interface

To enable source routing without spanning tree, use the following procedure.

1. **Select Source Routing from the Select Protocols menu and click on OK.**

   The Select Protocols menu appears after you either select a link or net module connector, or finish configuring a WAN circuit.

   The Edit Source Routing Global Parameters window appears (Figure 2-14).

2. **Specify the source routing bridge internal LAN ID and the source routing bridge ID, using the descriptions that follow as a guide.**

Note: Because source routing is global (that is, it runs across all Bridge circuits), the Configuration Manager only displays the Source Routing Global Parameters window the first time you specify source routing for the bridge. If this window does not appear, source routing is already enabled on the bridge.

Figure 2-14. Edit Source Routing Global Parameters Window

Parameter: **SR Bridge Internal LAN ID**

Default: 0x0

Range: 0x1 to 0xffe

Function: Specifies this bridge's internal LAN ID.

Instructions: Assign an internal LAN ID that is unique among all other internal LAN IDs, group LAN IDs, and ring IDs in the network.

You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.4

Parameter:	**SR Bridge ID**
Default:	0x0
Range:	0x1 to 0xf
Function:	Specifies this bridge's bridge ID and identifies the Bay Networks source routing bridges in the network.
Instructions:	Assign the same bridge ID to all Bay Networks source routing bridges in the network (unless two bridges operate in parallel; see note below). The bridge ID must be unique among any other non-Bay Networks bridge IDs in the network. You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.5

Note: If two Bay Networks source routing bridges operate in parallel, you must assign a different SR bridge ID to one of the bridges. You must also specify the SR bridge ID in the Bridge Entry list for all other Bay Networks source routing bridges in the network. (See "Implementation Notes" for more information.)

3. **When you have configured the required parameters in the Edit Source Routing Global Parameters window, click on OK.**

   The SR Interface List window appears (Figure 2-15).

4. **Specify the source routing ring number, using the description that follows as a guide, and click on OK.**

Figure 2-15. SR Interface List Window

Parameter: **Source Routing Ring Number**

Default: 0x0

Range: 0x001 to 0xfff

Function: Identifies the ring number (ring ID) of this source routing circuit.

Instructions: Assign a ring number (ring ID) to this source routing circuit that is unique among any other ring IDs, group LAN IDs, or internal LAN IDs in the network.

You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.6

Enabling Source Routing Spanning Tree Service on an Interface

To enable source routing spanning tree on an interface, complete the following steps:

1. **From the Select Protocols menu, select the Spanning Tree option that is directly under the Source Routing option.**

   Note that the Configuration Manager also selects the Source Routing option because this Spanning Tree protocol cannot run without source routing enabled.

   If you have not yet enabled source routing on any circuit, the Edit Source Routing Global Parameters window appears (Figure 2-14). If you have enabled source routing on some other circuit, the SR Interface List window appears (Figure 2-15).

   Refer to "Enabling Source Routing Services on an Interface" earlier in this chapter to configure the necessary source routing parameters.

2. **After you configure the interface parameters and click on OK in the SR Interface List window, the Source Route Spanning Tree Autoconfiguration window appears (Figure 2-16).**

Note: Because the spanning tree is global (that is, it runs across all source routing circuits), the Configuration Manager only displays the Source Route Spanning Tree Autoconfiguration window the first time you specify spanning tree for source routing. If you have previously specified spanning tree for source routing, this window will not appear.

Note: Although the parameters on this screen have the same names and functions as for spanning sree service under bridging, they need to be set independently for spanning tree service under source routing.

3. **Configure the Bridge Priority and Bridge MAC Address parameters, using the descriptions that follow as a guide.**

4. **When you have configured the required parameters, click on OK.**

   A pop-up window prompts

   ```
   Do you want to edit the Source Route Spanning Tree Interface Details?
   ```

5. **Click on Cancel to enable default spanning tree service and to display the next protocol-specific window, or click on OK to edit the default values.**

   Refer to "Editing Source Routing Parameters" for instructions.

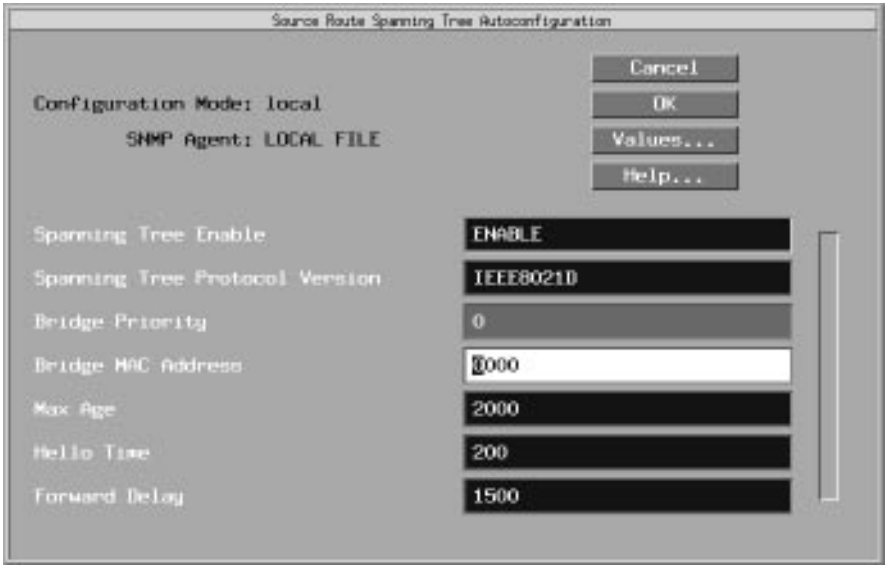


Figure 2-16. Source Route Spanning Tree Autoconfiguration Window

Parameter:	**Bridge Priority**
Default:	128
Range:	0 to 65535
Function:	Combined with the Bridge MAC Address parameter, assigns a 64-bit bridge ID to the router. This parameter supplies the most significant 16 bits of the bridge ID, while Bridge MAC Address supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest-number bridge ID. Thus, the lower the value of this parameter, the more likely that the router will be selected as the root bridge.
Instructions:	Enter a decimal value from 0 to 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.33

Parameter:	**Bridge MAC Address**
Default:	Defaults to a unique MAC address that the router automatically creates based on the router's backplane ID.
Options:	Any valid, 48-bit MAC-level address
Function:	Combined with the Bridge Priority parameter, assigns a 64-bit bridge ID to the router. Bridge Priority supplies the most significant 16 bits of the bridge ID, while this parameter supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest-number bridge ID. Thus, the lower the value of Bridge Priority, the more likely that the router will be selected as the root bridge. In the event of equal bridge priority values, the Bridge MAC Address value determines the bridge's priority.
Instructions:	Enter a 48-bit MAC address expressed as a 12-digit hexadecimal value. You should set this parameter to the MAC address of one of the router's spanning tree ports, preferably the one with the lowest priority.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.33

Editing Source Routing Parameters

Once you configure a circuit to support source routing, you use the Configuration Manager to edit the source routing parameters. This section provides information on how to access and edit these parameters.

Note: The instructions in this section assume that you have already configured source routing on the router. (Refer to “Enabling Source Routing Services” for details on configuring source routing.)

You access all source routing parameters from the Configuration Manager window (refer to Figure 2-17). Refer to *Using Site Manager Software* for details on accessing this window.

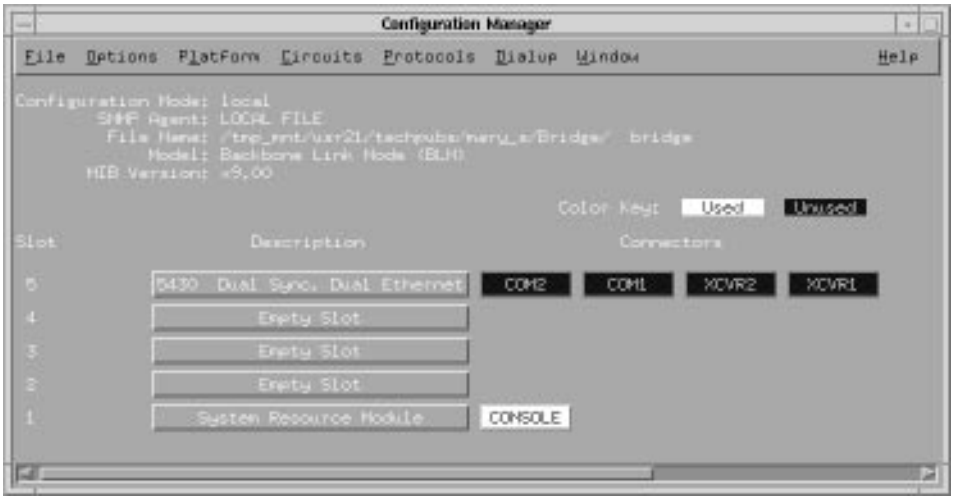


Figure 2-17. Configuration Manager Window

Editing Source Routing Global Parameters

To edit source routing global parameters:

1. **Select Protocols > Source Routing > Global in the Configuration Manager window (Figure 2-17).**

   The Edit Source Routing Global Parameters window appears (Figure 2-18).

Figure 2-18. Edit Source Routing Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**

   (Refer to 3 for details on editing the NetBIOS parameters.)

3. **Click on OK to save your changes and exit the window.**

Source Routing Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Source Routing Global Parameters window (Figure 2-18). Refer to Chapter 3 for details on configuring the NetBIOS parameters on this window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables source routing on the entire router.
Instructions:	Set to Disable if you want to disable source routing.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.2

Parameter:	**SR Bridge Internal LAN ID**
Default:	0x0
Range:	0x1 to 0xffe
Function:	Specifies this bridge's internal LAN ID.
Instructions:	Assign an internal LAN ID that is unique among all other internal LAN IDs, group LAN IDs, and ring IDs in the network. You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.4

Parameter:	**SR Bridge ID**
Default:	0x0
Range:	0x1 to 0xf
Function:	Specifies this bridge's bridge ID and identifies the Bay Networks source routing bridges in the network.
Instructions:	Assign the same value to all Bay Networks source routing bridges in the network (unless two bridges operate in parallel; see the following note). The SR bridge ID must be unique among any other non-Bay Networks bridge IDs in the network. You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.5

Note: If two Bay Networks source routing bridges operate in parallel, you must assign a different SR bridge ID to one of them. You must also specify the SR bridge ID in the Bridge Entry list for all other Bay Networks source routing bridges in the network. (See "Implementation Notes" for more information.)

Parameter:	**SR Bridge Group LAN ID**
Default:	0xfff
Range:	0x1 to 0xfff
Function:	Specifies this bridge's group LAN ID. The bridge uses the group LAN ID when transmitting specifically routed frames (SRFs) between Bay Networks bridges. Together with the other routing designators, the group LAN ID helps bridges manipulate the RIF.
Instructions:	Assign the same group LAN ID to all Bay Networks source routing bridges in the network. The group LAN ID must be unique among any other group LAN IDs, ring IDs, or internal LAN IDs in the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.6

Parameter:	**IP Encapsulation**
Default:	Disable
Options:	Enable | Disable
Function:	Enables IP encapsulation for those packets destined for an IP network.
Instructions:	Enable this parameter if the bridge borders an IP network cloud and you want to source-route frames across this IP network. If you enable this parameter, you must also configure the Conn. IP NTWK Ring number parameter for IP encapsulation to occur.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.7

Note: Refer to "Configuring IP Encapsulation Support" earlier in this chapter for details on IP encapsulation.

Parameter:	**Conn. IP NTWK Ring number**
Default:	0x0
Range:	0x1 to 0xffe
Function:	Identifies the ring ID of the IP network to which this bridge connects.
Instructions:	Assign the same value to all Bay Networks source routing bridges that border the IP network cloud. Make sure this value is unique among any other ring IDs, group LAN IDs, or internal LAN IDs in the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.8

Note: You cannot modify the Conn. IP NTWK Ring number parameter unless you first enable IP encapsulation. Refer to "Configuring IP Encapsulation Support" earlier in this chapter for details on IP encapsulation.

Parameter:	**IP MTU Size (bytes)**
Default:	4562
Range:	0 to 4562
Function:	Specifies the maximum MTU size for the IP network.
Instructions:	Select a value that equals the smallest MTU size of any of the links in the IP network. This allows the largest frame negotiation in the source routing exploration process to account for any link inside the IP cloud. You can accept the default value 4562. However, if you have links in your IP network with smaller MTU sizes than the default value, the IP entity may fragment packets. For maximum performance, refer to your network configuration and calculate this value based on actual MTU sizes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.11

Editing Source Routing Interface Parameters

To edit a source routing interface:

1. **Select Protocols > Source Routing > Interfaces in the Configuration Manager window (refer to Figure 2-17).**

   The SR Interface List window appears (Figure 2-19).

Figure 2-19. SR Interface List Window

2. **Select the interface you want to edit.**
3. **Edit the parameters, using the descriptions in the next section as a guide.**

   Refer to Chapter 3 for descriptions of the NetBIOS parameters on this screen.
4. **Click on Apply to save your changes.**
5. **Click on Done to exit the window. Site Manager returns you to the Configuration Manager window.**

Note: When you reconfigure an interface in dynamic mode, source routing restarts on that interface.

Source Routing Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the SR Interface List window (refer to refer to Figure 2-19). (Refer to Chapter 3 for descriptions of the NetBIOS parameters on this screen.)

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables source routing over this circuit.
Instructions:	Set this parameter to Enable to enable source routing over this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.2

Parameter:	**Max number of RDs**
Default:	7
Range:	1 to 7
Function:	Specifies the maximum number of route descriptors allowed in incoming explorer frames. Any explorer frames received that contain more route descriptors than specified here are dropped.
Instructions:	Accept the default unless you want to limit the number of networks this router can reach.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.5

Parameter:	**Source Routing Ring Number**
Default:	0x0
Range:	0x001 to 0xfff
Function:	Identifies the ring number (ring ID) of this source routing circuit.
Instructions:	Assign a ring number (ring ID) to this source routing circuit that is unique among any other ring IDs, group LAN IDs, or internal LAN IDs in the network. You cannot use the value 0x0 that appears initially in the parameter box. You must specify a value for this parameter that is within the given range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.6

Parameter:	**Outbound STEs**
Default:	Accept
Options:	Accept | Block
Function:	When set to Block, the bridge drops outbound STEs on this circuit. Use this parameter to configure a static spanning tree for spanning tree explorer packets. This parameter has no effect if you configure this interface with the Source Routing Spanning Tree protocol.
Instructions:	Set to Block only if you do not want the bridge to forward STEs on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.7

Note: Series 7 router software does not support dynamic source route spanning tree. You must statically configure which ports should accept or block STE frames. Series 8 router software does support dynamic source route spanning tree.

Parameter:	**Inbound STEs**
Default:	Accept
Options:	Accept | Block
Function:	Specifies whether the bridge should drop single route explorer frames received on this circuit. This option will not stop single route explorer frames from being transmitted on this circuit. This parameter has no effect if you configure this interface with the Source Routing Spanning Tree protocol.
Instructions:	Set to Block only if you want spanning tree explorer packets to be dropped by this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.8

Parameter:	**Frames with IP Ring**
Default:	Accept
Options:	Accept | Block
Function:	Specifies whether the bridge should block inbound explorer frames received on this circuit that traversed the IP network via IP encapsulation.
Instructions:	Set to Block only if you want to limit the route selection possibilities using IP encapsulation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.9

Parameter:	**IP Address**
Default:	None
Options:	Any valid IP address
Function:	Shows the IP address of this interface. (If there is no IP address, this field displays 0.0.0.0.) You can use this parameter with the IP Encapsulation parameter to map ring IDs to IP addresses.
Instructions:	If you accept the IP address displayed, then the ring ID maps to that address. If you want to change the ring ID mapping to the outgoing IP interface, enter 0.0.0.0 at this field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.10.

Note: If you did not configure IP on this interface already, the system will overwrite the value you entered for this parameter when you do configure IP.

Parameter:	**WAN Broadcast Address**
Default:	-1
Options:	Any valid Frame Relay data link connection identifier (DLCI) number
Function:	Sets the DLCI number this interface uses when it sends broadcast frames over Frame Relay.
Instructions:	Specify a DLCI number.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.23

Note: You cannot modify the WAN Broadcast Address parameter unless you first configure source routing over Frame Relay, ATM, or SMDS.

Parameter: **Encapsulation Format**

Default: Proprietary

Options: Proprietary | Standard

Function: Indicates Bay Networks proprietary encapsulation format or standard encapsulation format.

Instructions: If you want to run source routing over a Frame Relay network, follow these instructions:

- If your router, running software Version 8 or higher, communicates with a third-party router that supports RFC 1490, and you configured both routers to run source routing over Frame Relay, select Standard for RFC 1490 standard Frame Relay encapsulation.
- If your router, running software Version 8 or higher, communicates with a Version 5 Bay Networks router, and you configured both routers to run source routing over Frame Relay, accept the default, Proprietary.
- If your Version 8 router communicates with a Version 7 Bay Networks router, and you configured both routers to run source routing over Frame Relay, select Standard.
- If your router, running software Version 8 or higher, communicates with another Version 8 router, and you configured both routers to run source routing over Frame Relay, you can select either Proprietary or Standard; however, you must set the same encapsulation format for both routers.

If you want to bridge between source routing Token Ring and FDDI endstations, refer to the following instructions:

- If your router, running software Version 8 or higher, connects Token Ring endstations to FDDI endstations, select Standard for standard native encapsulation.
- If your router, running software Version 8 or higher, communicates with a third-party router via an FDDI network, and each router connects to a Token Ring network, select Standard.
- If your router communicates with a Version 5 or Version 7 router via an FDDI network, and each router connects to a Token Ring network, accept the default, Proprietary.
- If your router, running software Version 8 or higher, communicates with another router running Version 8 or higher via an FDDI network,

you can select either Proprietary or Standard; however, you must set the same encapsulation format for both routers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.24

Adding or Deleting a Bridge ID on the Bridge Entry List

You specify a bridge ID on the Bridge Entry list if you want to configure two or more Bay Networks source routing bridges in parallel. (Refer to "Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs" in this chapter for more information.) The following sections describe how to add and delete a bridge ID in the Bridge Entry list.

Adding a Bridge Entry to the Bridge Entry List

To add a bridge ID:

1. **Select Protocols > Source Routing > Bridge Entry in the Configuration Manager window (refer to refer to Figure 2-17).**

   The Source Routing Bridge IDs window appears, which lists the bridge IDs currently configured on the network (Figure 2-20).

Figure 2-20. Source Routing Bridge IDs Window

2. **Click on Add.**

   The Add Bridge ID window appears (Figure 2-21).

Figure 2-21. Add Bridge ID Window

3. **Enter the new bridge ID in the New Source Routing Bridge ID field, using the description in the next section as a guide.**
4. **Click on Add SR BR ID. Site Manager returns you to the Source Routing Bridge IDs window.**

   The bridge ID you configured now appears in the Bridge Entry list.

5. **Click on Done to exit the window. Site Manager returns you to the Configuration Manager window.**

Source Routing Bridge ID Parameter Description

Use this parameter description as a guide when you configure the parameter in the Add Bridge ID window (refer to Figure 2-21).

Parameter:	**New Source Routing Bridge ID**
Default:	None
Range:	1 to 15
Function:	Specifies the other active bridge IDs that exist on the network. This parameter is only necessary if you have parallel source routing bridges configured on your network.
Instructions:	Enter the bridge ID assigned to the parallel bridge on your network. Refer to "Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs" for details on parallel source routing bridges.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.3.1.1

Deleting a Bridge Entry from the Bridge Entry List

To delete a bridge ID:

1. **Select Protocols > Source Routing > Bridge Entry in the Configuration Manager window (refer to refer to Figure 2-17).**

   The Source Routing Bridge IDs window appears, which lists the other bridge IDs currently configured on the network (refer to Figure 2-20).

2. **Select a bridge ID from the list.**
3. **Click on Delete.**

   The bridge ID you deleted no longer appears in the Bridge Entry list.

4. **Click on Done to exit the window. Site Manager returns you to the Configuration Manager window.**

Adding or Deleting an IP Address on the IP Explorer Address List

You specify an IP address on the IP Explorer Address list if you want to source route across an IP network. The following sections describe how to add and delete an IP address in the IP Explorer Address list.

Adding an IP Explorer Address to the IP Explorer Address List

To add an IP explorer address:

1. **Select Protocols > Source Routing > Explorer Entry in the Configuration Manager window (refer to refer to Figure 2-17).**

   The Source Routing Bridge IP Explorer Addresses window appears (Figure 2-22), which lists the defined IP explorer addresses.

Figure 2-22. Source Routing Bridge IP Explorer Addresses Window

2. **Click on Add.**

   The Add Source Routing Explorer IP Address window appears (Figure 2-23).

Add Source Routing Explorer IP address
Enter Source Routing Bridge Explorer
New SR Bridge Explorer IP address
Add SR BR EXP
Cancel

Figure 2-23. Add Source Routing Explorer IP Address Window

3. **Enter the new IP address in the New SR Bridge Explorer IP address field, using the description in the next section as a guide.**
4. **Click on Add SR BR EXP.**

   Site Manager returns you to the Source Routing Bridge IP Explorer Addresses window.

   The IP address you configured now appears in the list.
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

IP Explorer Address Parameter Description

Use this parameter description as a guide when you configure the parameter in the Add Source Routing Explorer IP Address window (refer to refer to Figure 2-23).

Parameter:	**New SR Bridge Explorer IP address**
Default:	None
Options:	Any valid IP address.
Function:	Specifies a destination IP address that this bridge can use to source-route packets across an IP network.
Instructions:	Enter a valid destination IP address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.4.1.1

Deleting an IP Explorer Address

To delete an IP address from the IP Explorer Address list:

1. **Select Protocols > Source Routing > Explorer Entry in the Configuration Manager window (refer to refer to Figure 2-17).**

   The Source Routing Bridge IP Explorer Addresses window appears (refer to refer to Figure 2-22), which lists the defined IP explorer addresses.
2. **Select an IP address from the list.**
3. **Click on Delete.**

   The IP address you deleted no longer appears in the IP Explorer Address list.

4. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Editing Source Route Spanning Tree Global Parameters

To edit the source route spanning tree global parameters:

1. **Select Protocols > Source Routing > Spanning Tree > Global in the Configuration Manager window (refer to refer to Figure 2-17).**

   The Edit Source Route Spanning Tree Global Parameters window appears (Figure 2-24).

Figure 2-24. Edit Source Route Spanning Tree Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

Source Route Spanning Tree Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Source Route Spanning Tree Global Parameters window (refer to refer to Figure 2-24).

Parameter:	**Spanning Tree Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables spanning tree on the entire router.
Instructions:	Set to Disable if you want to disable spanning tree for the entire router, or to Enable if you want to re-enable spanning tree for the entire router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.30

Parameter:	**Spanning Tree Protocol Version**
Default:	IEEE8021D
Options:	IEEE8021D | Unknown | DECLB108
Function:	Specifies the version of the spanning tree protocol that the router is running.
Instructions:	Accept the default, IEEE8021D, or select one of the other options.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.32

Parameter:	**Bridge Priority**
Default:	128
Range:	0 to 65535
Function:	Combined with the Bridge MAC Address parameter, assigns a 64-bit bridge ID to the router. This parameter supplies the most significant 16 bits of the bridge ID, while Bridge MAC Address supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest-number bridge ID. Thus, the lower the value of this parameter, the more likely that the router will be selected as the root bridge.
Instructions:	Enter a decimal value from 0 to 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.33

Parameter:	**Bridge MAC Address**
Default:	Defaults to a unique MAC address that the router automatically creates based on the router's backplane ID.
Options:	Any valid, 48-bit MAC-level address
Function:	Combined with the Bridge Priority parameter, assigns a 64-bit bridge ID to the router. Bridge Priority supplies the most significant 16 bits of the bridge ID, while this parameter supplies the remaining (least significant) 48 bits. The spanning tree uses the bridge ID to select the root bridge. In selecting the root bridge, the spanning tree chooses the bridge with the lowest-number bridge ID. Thus, the lower the value of Bridge Priority, the more likely that the router will be selected as the root bridge. In the event of equal bridge priority values, the Bridge MAC Address value determines the bridge's priority.
Instructions:	Enter a 48-bit MAC address expressed as a 12-digit hexadecimal value. You should set this parameter to the MAC address of one of the router's spanning tree ports, preferably the one with the lowest priority.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.33

Caution: We recommend that you not change the following three spanning tree parameters (Max Age, Hello Time, and Forward Delay) unless absolutely necessary. However, if you do change them, you must follow these guidelines.

$$2 \times (\text{Forward Delay} - 1 \text{ Second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ Second})$$

BRG0010A

Note: If the values for Max Age, Hello Time, and Forward Delay are not the same for each bridge in your network, the root bridge parameters rule the entire topology.

Parameter:	**Max Age**
Default:	20 seconds (expressed in hundredths of a second: 2000)
Range:	6 to 40 seconds
Function:	Specifies the maximum number of seconds that the router considers protocol information (BPDUs) valid. After this specified amount of time, the router times out and discards the information. We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section.
Instructions:	Either accept the default value or specify a new value. Make sure to express any new value in hundredths of a second.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.43

Parameter:	**Hello Time**
Default:	2 seconds (expressed in hundredths of a second: 200)
Range:	1 to 10 seconds
Function:	Specifies the interval in seconds between BPDUs transmitted by the bridge. BPDUs are periodic transmissions exchanged between bridges in the network to convey configuration and topology change data. We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section.
Instructions:	Either accept the default value or enter a new value. Make sure you enter the new value in hundredths of a second.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.44

Parameter:	**Forward Delay**
Default:	15 seconds (expressed in hundredths of a second: 1500)
Range:	4 to 30 seconds
Function:	Specifies the time in seconds that a circuit spends in the listening and learning states. If you set this parameter to the minimum value, the spanning tree converges at its fastest rate. As the spanning tree algorithm operates, it eventually places all circuits in either a forwarding (enabled) or blocking (disabled) state. In response to network topology changes, the spanning tree algorithm may change the state of specific circuits. To prevent network looping caused by sudden state changes, the spanning tree algorithm does not transition circuits directly from the blocking to the forwarding state. Rather, it places them in two intermediate states: listening and learning. In the listening (standby) state, the circuit listens for network-generated BPDUs. It receives and drops all other traffic. When the forward delay timer expires, the spanning tree algorithm places the circuit in the learning state. In the learning state, the circuit receives both network-generated BPDUs, and endstation-generated traffic that is subjected to the learning process but is not relayed. When the forward delay timer expires, the spanning tree algorithm places the circuit in the forwarding state. We recommend that you accept the default, 15 seconds; however, if you change the value, you must follow the guidelines listed previously in this section.
Instructions:	Either accept the default value or enter a new value. Make sure you enter the new value in hundredths of a second.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.45

Editing Source Route Spanning Tree Interface Parameters

To edit the source route spanning tree interface parameters:

1. **Select Protocols > Source Routing > Spanning Tree > Interfaces in the Configuration Manager window (refer to Figure 2-17).**

   The Source Route Spanning Tree Interface List window appears (Figure 2-25).

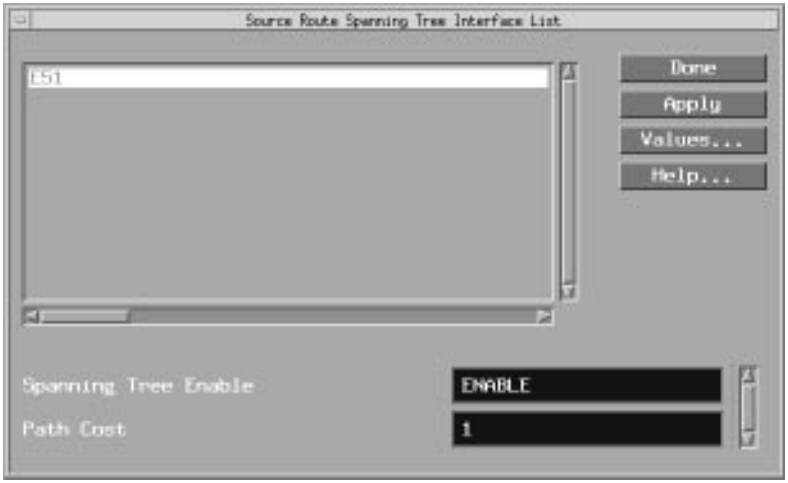


Figure 2-25. Source Route Spanning Tree Interface List Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes.**
4. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Source Route Spanning Tree Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Source Route Spanning Tree Interface List window (refer to refer to Figure 2-25).

Parameter: **Enable**

Default: If you added spanning tree using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable.

Options: Enable | Disable

Function: Toggles spanning tree on and off for this circuit only.

This parameter does not allow you to add spanning tree to this circuit. To add the spanning tree to this circuit, you must use the configuring-circuits procedure. For instructions, see *Configuring Routers*.

Instructions: Set this parameter to either Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.25

Parameter: **Path Cost**

Default: 1

Range: 1 to 65535

Function: When this port is the root port, the path cost is the contribution of the path through this port to the total cost of the path to the root for this bridge. When this port is *not* the root port, the router adds the path cost to the designated cost for the root port and uses it as the value of the root path cost offered in all configuration BPDUs transmitted by the bridge.

To determine the path cost, use this formula:

Interface Path Cost = 1000/Attached LAN speed in Mb/s

Instructions: Enter a path cost value for this interface in the Path Cost box. For example, enter 100 if the attached LAN is Ethernet (1000/10 = 100).

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.28

Deleting Source Routing from the Router

To delete source routing from all circuits on which you enabled it:

1. **Select Protocols** > **Source Routing** > **Delete Source Routing in the Configuration Manager window.**

   A confirmation window prompts

   ```
   Do you REALLY want to delete Source Routing?
   ```

2. **Select OK.**

   Site Manager returns you to the Configuration Manager window; source routing is no longer configured on the router.

Chapter 3
Using NetBIOS Services

This chapter provides

- An overview of the Network Basic Input/Output System (NetBIOS)
- Implementation notes you should consider before you attempt to customize NetBIOS
- Instructions for enabling NetBIOS
- Instructions on how to use the Configuration Manager to edit the NetBIOS parameters

NetBIOS Overview

NetBIOS is a standard mechanism for sharing services and information across a variety of transmission protocols and media.

NetBIOS Names

Each PC application that runs over a Token Ring LAN has a NetBIOS name. Applications use NetBIOS names to start and end sessions.

You can configure a single station with multiple applications, each of which has a unique NetBIOS name. Each PC that supports an application also has a NetBIOS station name that you assign or that NetBIOS derives by means internal to that station.

NetBIOS names can consist of up to 16 alphanumeric characters. The combination of characters must be unique within the entire source routing network.

You can configure the Bay Networks source routing bridge so that it treats NetBIOS names as though they have 15 characters. This feature is useful particularly in application environments that use the first 15 characters of the NetBIOS name to identify the station, and the last character to identify the application running on the station.

If the application uses source routing bridge name caching, it is more efficient to use only the first 15 characters. The resulting cache is smaller and the cache hits more common. If you do not know whether the applications use 15- or 16-character names, select 16-character names. Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of the 15-Character NetBIOS Name Caching parameter.

Registering Station Names

All NetBIOS stations advertise their names when they become active. A station is considered to be registered when it can successfully advertise its own name without any other station claiming it has the same name. The following steps describe how an application registers a station name.

1. To register itself on the network, a NetBIOS station sends *add name query* or *add group name query* frames for each name it wants to use. These frames contain each station's assigned name. The NetBIOS station repeats these commands typically six to ten times to increase the chance that all other stations hear them.
2. If another station already has the same name, that NetBIOS station issues an *add name response* command to indicate that the name is already in use. The station issuing the query must stop trying to use that name.
3. When a partitioned source route bridge network reconnects, two stations may have the same name. When a NetBIOS station detects this (for example, if it receives two or more *name recognized* responses to a *name query* request), it issues a *name in conflict* broadcast frame.
4. Upon receiving a *name in conflict* frame, the NetBIOS application using that name must stop trying to use that name. The application shuts down to eliminate the conflict.

Establishing Sessions

Once a NetBIOS application determines that its name is unique on the network, the application establishes a session with another NetBIOS application. The following steps describe how the application establishes the session.

1. The originating station sends out a NetBIOS *name query to determine the route to the destination application.* The query is a spanning tree explorer (STE) frame that invites a specific remote application to respond. (Refer to Chapter 2 for details on STE frames.)
2. As the *name query* STE frame propagates along its spanning tree route, the frame accumulates routing information field (RIF) data that traces its unique path through the loop-free topology of the network.
   - If you do not have a source routed spanning tree configured on your network, the STE propagates along all available routes to the destination application. Multiple copies of the *name query* STE frame may arrive at the destination station.
   - If your network has a spanning tree topology, only one copy of the *name query* STE frame arrives at the destination remote station.
3. The NetBIOS interface on the destination station recognizes the name of one of its own applications in the query frame. The NetBIOS interface responds by broadcasting a *name-recognized* all routes explorer (ARE) frame. (Refer to Chapter 2 for details on ARE frames.)
4. As the *name-recognized* ARE frame propagates toward the calling station along multiple paths, each frame accumulates RIF information that traces its unique path through the network. The originating source routing interface receives multiple copies of the *name-recognized* frame.
5. Depending on the number of parallel paths from the destination application back to the calling application, one or more copies of the *name-recognized* ARE response frame arrive at the originating station. The originating station accepts only the first *name-recognized* frame it receives, assuming that this frame contains the RIF for the shortest path to the destination station. The calling station uses this RIF for any subsequent frames sent to the destination station. All subsequent frames associated with the impending session are specifically routed frames (SRFs). (Refer to Chapter 2 for details on SRF frames.)

6. Based on the information gained from the *name-recognized* frame accepted by the originating application, the NetBIOS interface establishes a session directly between the originating and destination application. Once the session between applications is open, NetBIOS names are no longer necessary for the duration of that session.
7. When no further session transactions remain, the NetBIOS interface that serves the calling application closes the session.

Sessionless Communication

When a NetBIOS station wants to send information that does not require a response from the destination application, the local station transmits a NetBIOS *datagram* frame. The datagram allows the NetBIOS station to communicate without establishing a session. The source station or application can send a datagram as a broadcast frame or an SRF.

Broadcast Reduction

To increase the bandwidth available on your source routing network, the Bay Networks source routing bridge can convert broadcast frames (*add name query*, *add group name query*, *name-recognized query* response, and certain datagram frames) to specifically routed frames (SRFs). This process is called *broadcast reduction*.

You can customize the broadcast reduction capabilities of the source routing bridge, using these caching mechanisms:

- Name caching
  - -- Client name caching
  - -- Server name caching
  - -- Datagram RIF caching
- Query caching
- Cache lookup
- Cache aging

The following sections describe the functions of the caching mechanisms.

Name Caching

The source route bridge NetBIOS name cache contains NetBIOS names, MAC addresses and the RIF needed to reach the station containing that name.The NetBIOS name cache learns the station names from *name query* (if client cache is enabled), *name recognized* (if server cache is enabled), and datagram frames (if datagram cache is enabled). The name learned is always the source name of any given message.

If you enable any type of name caching, the router tries to convert any of the *name query*, *name recognized*, or datagram frames from an explorer to an SRF based on the destination name. Note that the router converts these frames regardless of the conditions under which it learned the frame's name.

For example, assume that there are three NetBIOS stations (A, B, and C) in the network and only server name caching is configured on the router.

- If Station A sends a *name query* frame for Station B, the router does not cache any names.
- When Station B responds with a *name recognized* frame, the router caches Station B's name, MAC address, and RIF, but it does not convert the *name recognized* frame to an SRF because Station A is not in the cache.
- If Station C now sends a datagram to Station B, the router converts it to an SRF using the cache (even though datagram caching is disabled).

Note that the enabling or disabling of caching refers to the learning of names, not to the conversion of AREs to SRFs. The router tries to convert AREs to SRFs on *name query*, *name recognized*, and datagram requests whenever any type of name caching is enabled.

Client Name Caching

If you enable client name caching, the source routing bridge caches (learns and stores in the NetBIOS name cache tables) the source name and associated RIF found in any *name query* STE frame it receives. In addition, the source routing bridge uses information cached from *name query* frames to convert *name recognized*, datagram, or other *name query* broadcast frames into SRFs.

If you disable client name caching, the source routing bridge cannot cache client names and RIFs.

For optimal efficiency, you should use client name caching on the routers that are nearest to the servers. In this configuration, the router converts frames originated from the servers and destined for the clients from AREs to SRFs as early as possible along the path back to the client. Since there may be a large number of clients on the network, the client name cache could grow quite large. Therefore, be sure to observe available memory on the router when using this feature.

The primary function of client name caching is to convert *name recognized* frames from AREs to SRFs. You can configure the client name cache to age entries quickly because the *name recognized* frame is typically returned to the server, soon after the *name query* is sent and because clients may be powered off or moved around the network. Quicker aging of the client name cache may help reduce the need for large amounts of memory in the router.

Server Name Caching

If you enable server name caching, the source routing bridge caches the source name and associated RIF found in any *name-recognized* broadcast frame it receives. In addition, the source routing bridge uses information cached from *name-recognized* broadcast frames to convert *name query*, datagram, or other *name query* STE explorer frames into SRFs.

If you disable server name caching, the source routing bridge cannot cache server names and RIFs.

For optimal efficiency, you should enable server name caching on the routers that are nearest to the clients. In this configuration, the router converts frames originating from the clients and destined for the servers from AREs to SRFs as early as possible along the path to the server. Server name caching also reduces the number of broadcasts from multiple clients trying to reach the same server. As a general rule, server name caching consumes less memory than client name caching, because a network usually has fewer servers than clients. You can usually configure the server cache for a longer aging interval than the client cache, because servers tend to be less mobile than clients.

Datagram RIF Caching

If you enable datagram name caching, the source routing bridge caches the source name and associated RIF found in any datagram frame it receives. In addition, the source routing bridge uses information cached from datagram broadcast frames to convert broadcast *name query, name recognized*, or other datagram frames into SRFs.

If you disable datagram name caching, the source routing bridge cannot cache NetBIOS names and RIFs that it receives in datagrams.

Query Caching

When a NetBIOS station comes up on the network, it may rebroadcast *add name query* and *add group name query* frames five to ten times at 0.5-second intervals. This increases the probability that all NetBIOS stations eventually receive these frames.

The NetBIOS query cache is completely independent of the name cache. Its purpose is to filter redundant *add name query* and *add group name query* requests. The NetBIOS query cache captures the first *add name* or *add group name query* frame it receives. The router then compares any *add name* or *add group name query* frame it receives subsequently to all of the *add name* and *add group name query* frames held in cache.

If the received query matches any cached query, the router immediately discards or drops the received query. The query cache, therefore, prevents duplicate *add name query* or *add group name query* frames from flooding the network repeatedly. Query caching benefits all sizes of networks, especially larger NetBIOS environments.

The query caching mechanism also prevents duplicate *status query* frames from flooding the network.

You can adjust the maximum number of entries allowed in the query cache, using the source routing bridge's Max Number Query Cache Entries global parameter. Any adjustments you make affect the number of queries that each slot can monitor.

You can also configure the router to create or disable a MIB instance for each NetBIOS query held in the query cache, using the Create MIB Instances for Cached Name global parameter. When you enable this function, you can use SNMP GET commands to view entries in the query cache table in the MIB. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.)

Query caching consumes approximately 100 bytes per entry. Each cache entry remains in the query cache for a short time (approximately 3 seconds). However, if the number of NetBIOS stations and applications in your network is large, you may want to leave the query cache MIB function disabled to enhance router performance.

Cache Lookup

The source routing bridge uses a table lookup process for name searching, which uses a fast-string hash and search mechanism. You can use the Hash Entry Count global parameter to adjust the number of entries in the hash table. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.)

When you increase the number of entries in the hash table, you

- Decrease the likely number of names the router must compare before it finds a specific cached name.
- Decrease the amount of time it takes the router to find a particular cached name.
- Increase memory usage.

Note that when you increase the number of entries in the hash table, you do not increase the number of names that the router can cache. You determine the number of names using the Max Number Query Cache Entries global parameter. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.)

When you decrease the number of entries in the hash table, this generally produces an opposite effect on the cache lookup mechanism.

Cache Aging

The router ages name cache and query cache entries to ensure that cached routes remain consistent with the current network topology. If the cache table lookup mechanism does not access a cache entry within the interval you set in the appropriate cache aging time parameter, the router deletes the entry from the table.

You can adjust the aging time for the name/RIF cache using the Name Cache Age parameter, which is a source routing bridge global parameter. Any adjustments you make affect all instances of the source routing bridge in the router configuration.

You can adjust the aging parameter for the query cache by means of the NetBIOS Query Cache Age parameter, which is also a global parameter of the source routing bridge.

Refer to NetBIOS Global Parameter Descriptions for descriptions of the Cache Age Time and NetBIOS Query Cache Age parameters.

Statically Configured NetBIOS Names

You can add static NetBIOS names and associated RIF entries into the router. These entries are independent of the name and RIF entries learned dynamically in the name cache.

The static RIF must reflect a valid learned route. Since specifying a valid RIF is a complicated procedure, we recommend that you copy a RIF that the router learned dynamically into the name cache.

Implementation Notes

The following sections contain information you may need to know before you configure NetBIOS on the router.

Topologies

If you configure your source routed network to operate as a spanning tree, this may affect the client name caching feature. The following sections describe the effects on client name caching when you have a spanning tree or other topology.

Spanning Tree Topology

If you configure the source route network as a spanning tree, you should disable client name caching, because clients typically send *name query* frames as spanning tree explorers (STEs). Unless you disable client name caching, the client learns only about the spanning tree path to the server. This creates excess traffic on the spanning tree links and reduces the overall performance of the network.

By disabling client name caching when the source route network is configured as a spanning tree, *name recognized* broadcast frames can propagate back along all paths from the server to the querying client. The first frame that arrives at the client presents the best route to the destination applications.

You can use server name caching regardless of whether a source route spanning tree exists, because the router learns server names from *name recognized* frames which are typically sent as AREs.

Whether or not to use datagram caching in a source route spanning tree network depends on whether the particular applications are using AREs or STEs in their datagrams. In general, if the application sends datagrams as STEs, you should disable datagram caching.

Other Topologies

If your network design goals do not allow for a spanning tree topology, you can enable or disable client name caching, as needed, to suit the performance requirements of that network and the applications that run on it.

NetBIOS Caches

If you use data link switching (DLSw) and source route bridge NetBIOS on the same network, the source route bridge NetBIOS does not convert frames from broadcast to SRF frames. However, if multiple source route interfaces exist, you may use source route bridge NetBIOS caching to convert from broadcast to SRF frame.

The source route bridge and DLSw interfaces each have NetBIOS caches, but they operate independently for each protocol. The source route bridge NetBIOS caches hold the RIFs associated with clients or servers on LAN segments attached to the local router. The DLSw NetBIOS cache holds the IP addresses associated with DLSw peers configured on remote routers.

Refer to *Configuring DLSw Services* for details on DLSw services.

Enabling NetBIOS Services

This section describes how to enable NetBIOS services under source routing. It assumes you have followed the directions in Chapter 2 to enable source routing services.

To enable NetBIOS under source routing, open the Edit Source Routing Global Parameters window (Figure 3-2) and change the default values of the NetBIOS global parameters, as described in the following sections. Note that by default NetBIOS is enabled on all interfaces. To disable NetBIOS on one or more interfaces, edit the NetBIOS Interface parameters in the SR Interface List (Figure 3-3) window as described in the following sections.

Refer to Chapter 2 for details on editing the source routing global parameters in these windows.

Editing NetBIOS Parameters

Once you configure a circuit to support source routing, you use the Configuration Manager to edit the NetBIOS parameters. This section describes how to access and edit these parameters.

Note: The instructions in this section assume that you already configured source routing on the router. If you did not, refer to *Configuring Routers* for details on configuring source routing.

You access all NetBIOS parameters from the Configuration Manager Window (Figure 3-1). (Refer to *Using Site Manager Software* for details on accessing this window.)

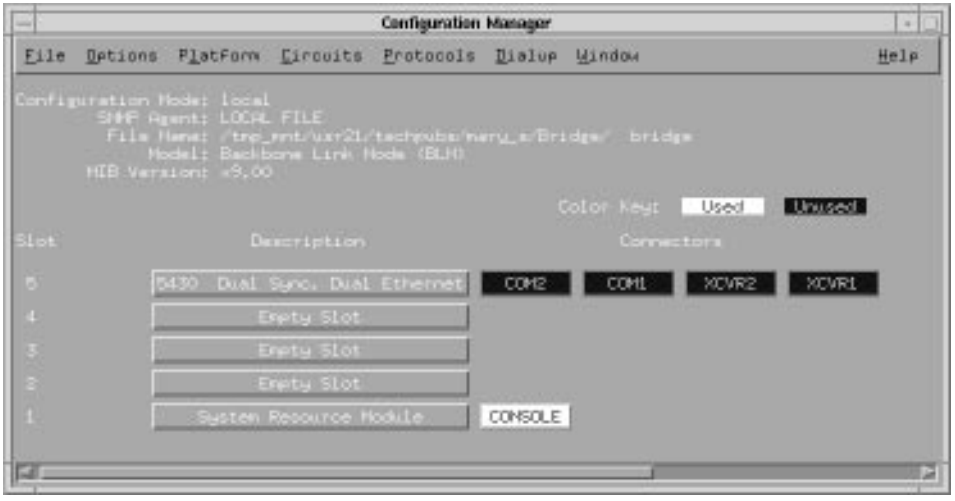


Figure 3-1. Configuration Manager Window

For each NetBIOS parameter, this section describes default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Editing NetBIOS Global Parameters

To edit the global NetBIOS parameters:

1. **Select Protocols > Source Routing > Global from the Configuration Manager window (refer to Figure 3-1).**

   The Edit Source Routing Global Parameters window appears (Figure 3-2).

Figure 3-2. Edit Source Routing Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**

   (Refer to Chapter 2 for details on editing the source routing parameters.)

3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

NetBIOS Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the NetBIOS parameters on the Edit Source Routing Global Parameters window (refer to Figure 3-2). (Refer to Chapter 2 for details on editing the source routing global parameters on this window.)

Parameter:	**NetBIOS Server Name Cache**
Default:	Disable
Options:	Enable | Disable
Function:	Globally enables or disables the ability of bridges to cache the source name, MAC address, and RIF path associated with each NetBIOS server that is active on the network.
Instructions:	Select Enable to activate NetBIOS server name, address, and RIF caching at every source routing interface configured on the node.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.12

Parameter:	**NetBIOS Client Name Cache**
Default:	Disable
Options:	Enable | Disable
Function:	Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS client that is active on the network.
Instructions:	Select Enable to activate NetBIOS client name, address, and RIF caching at every source routing interface configured on the node. Accept the default (Disable) if your network has a spanning tree topology.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.13

Parameter:	**NetBIOS Datagram RIF Cache**
Default:	Disable
Options:	Enable | Disable
Function:	Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS datagram handled by the node.
Instructions:	Select Enable to activate NetBIOS datagram source name, address, and RIF caching at every source routing interface configured on this node.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.14

Parameter:	**15-Character NetBIOS Name Caching**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables the ability of bridges to treat NetBIOS names either as 15- or 16-character entities.
Instructions:	Select Enable to activate 15-character NetBIOS name caching at every source routing interface configured on this node. Select Disable if you want NetBIOS to treat names as 16-character entities.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.15

Parameter:	**Create MIB Instances for Cached Name**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the ability of the system to – Create a MIB instance for each name entry stored in the name cache. – Delete a MIB instance for each NetBIOS name entry that ages out of the name cache.
Instructions:	Select Disable if you want to release the system memory and processing resources otherwise dedicated to maintaining cached names in the MIB.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.16

Parameter:	**Max Name Cache Entries**
Default:	100
Range:	1 to 2147483648
Function:	Specifies the maximum number of entries you need to provide in the NetBIOS name and RIF cache. The default value, 100, is a value suitable for networks that include up to 100 NetBIOS station names to cache. You can adjust the value of this parameter in direct proportion to the total number of client and server names expected to be active during intervals of peak traffic load or performance demand on the router.
Instructions:	Accept the default value or select a value suitable for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.17

Parameter:	**Name Cache Age (secs)**
Default:	300 seconds
Range:	1 to 2147483648 seconds
Function:	Specifies the interval (in seconds) after which inactive NetBIOS names, addresses, and RIFs expire from the NetBIOS Name Cache. Choose an aging value that allows infrequently referenced or obsolete client and server names, addresses, and RIFs to expire and be deleted from the name cache. The smaller the value, the less efficient broadcast reduction is, but the more quickly the network recovers from source routing topology changes.
Instructions:	Accept the default value or enter a new value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.19

Parameter: **Hash Entry Count**

Default: 253

Range: 253 to 2147483648

Function: Specifies the number of entries you want to allow in the hash tables.

Instructions: Increasing the number of hash table entries does not increase the number of names that a bridge can cache. With larger networks, increasing the size of the hash tables may, however, reduce internal cache lookup time, thereby improving overall performance.

Within each hash table entry, names are searched linearly. To increase performance, reduce the number of names in each hash table entry. The larger the number of hash table entries, the more likely that fewer names will hash into each entry.

Selecting a larger hash entry count consumes only slightly more memory (only 4 bytes per hash table entry). Therefore, you can increase performance by selecting a hash entry count that is a prime number close to 1/3 or 1/4 the total number of unique NetBIOS names active in the network. Using a prime number (for example, 253) is important to improve the chances of NetBIOS names hashing more evenly into the hash entries.

For networks that actively use up to 2500 NetBIOS client and server names, use the value 253. To determine a Hash Entry Count for larger networks:

- Divide the total number of unique NetBIOS client and server names active in the network by 10.
- Adjust the quotient to the nearest (higher or lower) prime number. (A prime number can only be divided by itself or 1 and still yield a whole-number quotient.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.20

Parameter:	**NetBIOS Query Cache**
Default:	Disable
Options:	Enable | Disable
Function:	Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS *add name query* and *add group name query* handled by the node.
Instructions:	Select Enable to allow source routing bridge interfaces to store names, addresses, and RIF paths associated with each NetBIOS query.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.24

Parameter:	**Create MIB Instances for Cached Query**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the ability of the system to – Create a MIB instance for each NetBIOS query stored in the query cache. – Delete a MIB instance for each NetBIOS query that ages out of the query cache.
Instructions:	Select Disable if you want to release system memory and processing resources otherwise dedicated to maintaining this MIB function.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.25

Parameter:	**Max Number Query Cache Entries**
Default:	100
Range:	1 to 100
Function:	Specifies the maximum number of entries allowed in the NetBIOS query cache. You can adjust the value of this parameter in direct proportion to the total number of NetBIOS stations that start up during intervals of peak traffic load or performance demand on the router.
Instructions:	Accept the default value or enter a vlue suitable for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.26

Parameter:	**NetBIOS Query Cache Age (secs)**
Default:	15 seconds
Range:	1 to 2147483648 seconds
Function:	Specifies the interval (in seconds) after which inactive or obsolete NetBIOS name queries are deleted from the query cache. The value 100 enables the router to hold (in query cache) the names, addresses, and RIF paths captured from up to 100 unique NetBIOS name query packets. Choose a query cache aging time that ensures that name queries that are either dormant or contain obsolete RIFs, do not unnecessarily occupy the NetBIOS query cache. Since a NetBIOS station typically transmits a query frame for 3 seconds, the default value should be sufficient.
Instructions:	Accept the default value or enter a new value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.1.28

Editing NetBIOS Interface Parameters

To edit NetBIOS interface parameters:

1. **Select Protocols > Source Routing > Interfaces from the Configuration Manager window (refer to Figure 3-1).**

   The SR Interface List window appears (Figure 3-3).

Figure 3-3. SR Interface List Window

2. **Select the interface you want to modify.**
3. **Edit the parameters, using the descriptions in the next section as a guide.**

   (Refer to Chapter 2 if you want to edit the source routing interface parameters.)
4. **Click on Apply to save your changes.**
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

NetBIOS Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the SR Interface List window (refer to Figure 3-3). (Refer to Chapter 2 for details on editing the source routing interface parameters on this window.)

Parameter: **NetBIOS Server Name Cache**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the ability of this bridge interface to cache the source name, MAC address, and RIF path for each NetBIOS server active on the network.

Instructions: Select Enable if you disabled server name caching previously, and you want to re-enable it.

Select Disable if you want to release system memory and processing resources otherwise dedicated to server name caching.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.17

Parameter: **NetBIOS Client Name Cache**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the ability of this bridge interface to cache the source name, MAC address, and RIF path for each NetBIOS client active in the network.

Instructions: Select Enable if you disabled client name caching previously, and you want to re-enable it.

Select Disable if you want to release system memory and processing resources otherwise dedicated to client name caching.

Select Disable if your network has a spanning tree topology.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.18

Parameter:	**NetBIOS Datagram RIF Cache**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the ability of this bridge interface to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS datagram handled by the bridge.
Instructions:	Select Enable if you disabled datagram caching previously, and you want to re-enable it. Select Disable if you want to release system memory and processing resources otherwise dedicated to datagram caching.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.19

Parameter:	**NetBIOS Query Cache**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the ability of this bridge interface to cache NetBIOS queries.
Instructions:	Select Enable if you previously disabled name query caching on this interface, and you want to re-enable it. Select Disable if you want to release system memory and processing query resources otherwise dedicated to caching.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.2.1.20

Using Statically Configured NetBIOS Clients and Servers

The following sections describe how to add, edit, and delete statically configured NetBIOS clients and servers; refer to the appropriate section.

Adding a Statically Configured NetBIOS Client or Server

You may want to statically configure NetBIOS names that are stable elements of your network configuration. When you statically configure a name, it reduces the use of system memory and processing resources normally required for learning and maintaining the NetBIOS names, MAC addresses, and RIFs associated with those names.

To add a statically configured NetBIOS name:

1. **Select Protocols > Source Routing > NetBIOS Static Name from the Configuration Manager window (refer to Figure 3-1).**

   The NetBIOS Static List window appears (Figure 3-4).

Figure 3-4. NetBIOS Static List Window

2. **Click on Add.**

   The NetBIOS window appears (Figure 3-5).

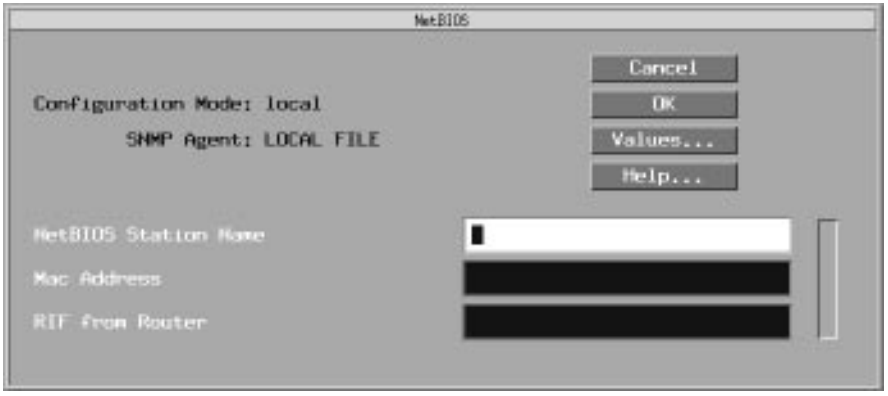


Figure 3-5. NetBIOS Window

3. **Enter values for the parameters, using the descriptions in the next section as a guide.**
4. **Click on OK to save your changes.**
5. **Click on Done to exit the window.**

   Site Manager returns you to the NetBIOS Static List window. (Refer to the next section to edit the parameters on this window.)

Static Name Parameter Descriptions

Use these parameter descriptions as a guide when you configure parameters in the NetBIOS window (refer to Figure 3-5).

Parameter:	**NetBIOS Station Name**
Default:	None
Options:	Any valid NetBIOS name
Function:	Specifies a NetBIOS name you want to add to the list of statically configured names that this node can reach.
Instructions:	Enter the NetBIOS name you want to add. The name must not exceed 16 characters. The system pads names shorter than 16 characters with ASCII space characters (0x20).
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.4

Parameter:	**Mac Address**
Default:	None
Options:	Any valid, 48-bit MAC address
Function:	Specifies the MAC address of the NetBIOS name you want to add to the list of statically configured names that this node can reach.
Instructions:	Enter the valid, 48-bit (6-byte) MAC address of a NetBIOS client or server this node must reach.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.5

Parameter:	**RIF from Router**
Default:	None
Options:	Any valid RIF, with entries specified in hexadecimal format
Function:	Specifies the RIF required for any frame to reach the NetBIOS name you want to add.
Instructions:	After you add a NetBIOS name to the static list, specify the RIF from the router to the station that uses the name. First, allow the bridge to use the route discovery process to learn the correct RIF of the station. You can use the Quick Get function accessible from Site Manager's Statistics Manager tool to examine the RIF by requesting the MIB object wfBrSrNbRifEntry.wfBrSrNbRif. (Refer to *Managing Routers and BNX Platforms* for instructions on using the Statistics Manager tool.) Next, copy the RIF to this RIF from Router parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.6

Editing Statically Configured NetBIOS Clients and Servers

To edit statically configured NetBIOS clients and servers:

1. **Select Protocols > Source Routing > NetBIOS Static Name in the Configuration Manager window (refer to Figure 3-1).**

   The NetBIOS Static List window appears, which lists all of the statically configured NetBIOS clients and servers currently defined in the node configuration (refer to Figure 3-4).

2. **Select the static entry you want to modify.**
3. **Edit the parameters, using the descriptions in the next section as a guide.**
4. **Click on Apply to save your changes.**
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

NetBIOS Static List Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the NetBIOS Static List window (refer to Figure 3-4).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables caching of the NetBIOS name you selected.
Instructions:	Select Enable to activate caching of the name you selected. Select Disable to deactivate caching of the name you selected.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.2

Parameter:	**Mac Address**
Default:	None
Options:	Any valid, 48-bit MAC address
Function:	Specifies the MAC address of the NetBIOS name you selected.
Instructions:	Specify the MAC address of the name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.5

Parameter:	**RIF from Router**
Default:	None
Options:	Any valid RIF, with route entries specified in hexadecimal format
Function:	Specifies the RIF required for any frame to reach the NetBIOS station you selected.
Instructions:	After you add a NetBIOS name to the static list, specify the RIF from the router to the station that uses the name. First, allow the bridge to use the route discovery process to learn the correct RIF of the station. You can use the Quick Get function accessible from Site Manager's Statistics Manager tool to examine the RIF by requesting the MIB object wfBrSrNbRifEntry.wfBrSrNbRif. (Refer to *Managing Routers* for details on using the Statistics Manager tool.) Next, copy the RIF to this RIF From Router parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.10.1.6

Deleting a Statically Configured NetBIOS Name

To delete a statically configured NetBIOS name:

1. **Select Protocols > Source Routing > NetBIOS Static Name from the Configuration Manager window (refer to Figure 3-1).**

   The NetBIOS Static List window appears, which lists all of the statically configured NetBIOS clients and servers currently defined in the node configuration (refer to Figure 3-4).

2. **Select the NetBIOS name you want to delete.**

3. **Click on Delete.**

The system deletes the entry you selected and removes it from the list of NetBIOS names in the NetBIOS Static List window.

Chapter 4
Using Translation Bridge Services

This chapter contains

- An overview of the transparent-to-source routing translation bridge (referred to as the *translation bridge* in this chapter)
- Implementation information you should know before you use the translation bridge
- Instructions for operating the translation bridge
- Descriptions of translation bridge parameters and instructions for editing those parameters

Translation Bridge Overview

One type of network uses a technique called *source routing* (SR) to bridge frames across networks. In SR networks, the station that transmits a frame includes, as part of the frame, the route that frame should traverse. The station learns the route through a route-discovery process. (Refer to Chapter 2 for details on source routing bridge services.)

Another type of network uses a technique called *transparent bridging* (TB) to link networks. In a TB network, the bridge builds a database of node addresses to determine when it should forward or drop frames; the endstations on TB networks are not aware of forwarding routes. (Refer to Chapter 1 for details on transparent bridge services.)

The translation bridge provides a method of bridging these two kinds of networks. This allows endstations using different bridging techniques to communicate as though they use the same bridging technique.

Databases

To connect the TB and SR networks, the translation bridge uses two databases. The following sections describe each database.

Forwarding Database

The translation bridge adds addresses to the forwarding table as it learns them from the network. Therefore, the forwarding table size should be configured large enough to hold the addresses it learns from both the TB network and the SR network.

Both the transparent bridge and the translation bridge use the same forwarding table to make decisions on where to send packets. The following sections discuss how the translation bridge makes these decisions.

Route Information Field Database

The *route information field database* includes routing information for all known stations on the network. The translation bridge uses this database to provide source routing information for frames it forwards from the TB network to the SR network.

When the translation bridge learns an address on the SR network, it adds the RIF information to the RIF database and adds the address and port information to the forwarding database. When the TB network forwards a frame to the SR network, the forwarding database determines the correct port to be used to reach the destination. The RIF database determines the correct RIF to insert in the frame so it can successfully traverse the SR network.

Database Aging Mechanism

The information that the translation bridge inserts into the forwarding database and the RIF database has an aging attribute that determines how long the information remains in the databases. Each time the translation bridge receives a frame from a particular SR station address, the age in both databases is reset. When the aging attribute reaches a user-configurable value, the translation bridge deletes the entries for that SR station from both the RIF database and the forwarding database. This aging mechanism allows you to control how quickly the translation bridge adapts to changes in the SR network topology.

Bridge Operations

The Bay Networks translation bridge software provides a link between the transparent bridging and source routing software on the router. The following sections describe how that link functions.

SR Operations

To facilitate SR operations, you assign the TB network a *ring number*. To stations on the SR network, the entire TB network appears to be one additional network segment or ring, identified by this ring number. When the SR bridge receives a frame destined for this ring number, it passes it to the translation bridge.

Routing of Explorer Frames

SR networks use explorer frames to determine the route between stations. (Refer to Chapter 2 for a description of how SR networks determine routes.)

Some stations generate all-routes explorer (ARE) frames, which are multiple frames that traverse all the possible routes between source and destination endstations. Some stations generate a spanning-tree explorer (STE) frame, a single frame that follows a loop-free path from source to destination.

When an SR network interface receives an STE or ARE explorer frame, the source route bridge is responsible for forwarding that frame to any other appropriate source route network interfaces. The translation bridge is responsible for forwarding that frame to any other appropriate transparent bridge network. When the translation bridge receives either an STE or ARE explorer frame, it determines what to do based on the frame's source and destination addresses, as follows:

- If the frame has a group destination address, the translation bridge completes these steps:
  - -- Forwards the frame to the transparent bridge, which sends it out all ports.
  - -- If the source address is not in the RIF table, adds the address and its routing information to the table.
  - -- If the source address is in the RIF table, updates its routing information.
- If the frame has a specific destination address, the translation bridge completes these steps:
  - -- If the source address is not in the RIF table, adds the address and its routing information to the table.

-- If the source address is in the RIF table, updates its routing information.

-- If the destination address is in the RIF table, discards the frame since it is intended for an SR station.

-- If the destination address is not in the RIF table or the forwarding table, converts the frame and sends it out all other TB ports.

Routing of Specific-Route Frames

Once an endstation on the SR network determines the route between itself and another endstation by sending out explorer frames, it can send a frame destined for that other endstation. This frame is a specifically routed frame (SRF). If the SR bridge receives an SRF that includes the ring ID of the TB network in its routing information, the SR bridge forwards the frame to the translation bridge. The translation bridge completes these steps:

- If the destination address exists in the forwarding table, the translation bridge converts the frame and forwards it to the appropriate TB network interface. If the destination address is not in the forwarding table, the translation bridge converts the frame and floods it to all TB network interfaces.
- If the SRF's source address is not already in the RIF table, the translation bridge adds it to the database and stores its routing information.

TB Operations

When the transparent bridge receives a frame from a TB network, it determines what to do based on the frame's source and destination address, as follows:

- If the source address is not in the forwarding table, the transparent bridge adds it.
- If the destination address is in the forwarding table as a station on a TB network, the transparent bridge sends the frame to the appropriate TB port.
- If the destination address is in the forwarding table as a station on an SR network, the transparent bridge forwards the frame to the translation bridge. The translation bridge then converts the frame, adds its routing information from the RIF table, and forwards the frame to the appropriate SR port.

- If the destination address is not in the forwarding table, the transparent bridge forwards the frame out all other TB ports and to the translation bridge. The translation bridge converts the frame and sends it to the SR network as either an STE or ARE frame, depending on how you configured the translation bridge software. (Refer to the next section for details on configuring the translation bridge software for STE or ARE frames.)

Note: An ARE or STE frame includes the ring ID of the TB network in the route information field.

Configuring for STE or ARE Frames

When the translation bridge software forwards a frame with an unknown destination address onto the SR network, it sends the frame as either an STE or ARE frame. By default, the translation bridge uses STE frames, so it does not overload the SR network with excessive ARE traffic. However, when the translation bridge sends STE frames, all of the traffic between the TB and SR networks follows the spanning-tree route through the SR network; this may not be the optimal route.

If you connect TB networks across a large SR network, you may want to configure the translation bridge to forward frames as ARE frames. This allows the frames to follow routes other than the spanning-tree route across the SR LAN.

TB to SR Challenges

The translation bridge software must overcome differences in the way that TB and SR networks implement various aspects of data transmission. These differences include

- Frame formats
- Frame lengths
- MAC address formats
- LAN speed

The following sections describe how the translation bridge software accommodates these differences.

Frame Format Selection

The Ethernet Version 2 and Ethernet 802.3 protocols transmit data using different formats for frames. For example, in Ethernet Version 2, the first section of the frame (the *preamble*) requires eight octets. For Ethernet 802.3 frames, the preamble is seven octets long. The translation bridge converts the frames it receives from the SR network to either Ethernet Version 2 or Ethernet 802.3 format. Then the translation bridge sends the frames to the transparent bridge for forwarding.

When you configure the translation bridge, you select a default conversion, either Ethernet 802.3 or Ethernet Version 2. When the translation bridge receives a frame from the SR network, it converts the frame to the format you specified as the default. You can specify exceptions to the default so that frames destined for certain endstations use the other frame format.

Frame Lengths

SR and TB networks often use different maximum frame lengths. For example, Ethernet networks support a maximum transmission unit (MTU) size of 1500 bytes, while Token Ring networks support much larger MTUs.

To resolve these differences, the translation bridge software specifies a maximum size of 1470 in the largest-frame-size bits of the routing information field on all frames forwarded to the SR network. The translation bridge cannot forward frames it receives from the SR network that are larger than 1500 bytes.

MAC Address Formats

Ethernet networks transmit the least significant bit of each byte of a MAC address first, while Token Ring networks transmit the most significant bit first. The translation bridge, therefore, reverses the bits in the source and destination addresses in the header of each frame it transfers between Ethernet and Token Ring networks. You can also define explicit mappings between Ethernet group addresses and Token Ring functional addresses. (Refer to "Editing Translation Bridge MAC Address Conversions" later in this chapter for details about MAC address conversions.)

LAN Speeds

When the translation bridge transfers frames between networks that have different network speeds, the software automatically accommodates for variations in throughput. If the difference in speeds is significant, the translation bridge may drop some frames.

Implementation Notes

The following sections contain specific information you should know before you use the Bay Networks translation bridge.

Protocols Supported

The translation bridge supports the transfer of logical link control-based (LLC) traffic. You can designate the service access points (SAPs) that the translation bridge accepts. By default, the translation bridge accepts traffic destined for NetBIOS (0xF0), Systems Network Architecture (SNA) (0x04, 0x08, 0xFC), and LAN Network Manager (LNM) SAPs (0xF4).

Interfaces Supported

The translation bridge can operate on all TB interfaces supported by the Bay Networks router, including

- Ethernet/802.3
- Fiber Distributed Data Interface (FDDI)
- Bay Networks serial
- Frame Relay
- Switched Multi-Megabit Data Service (SMDS)
- Point-to-Point Protocol (PPP)
- Token Ring encapsulation

The translation bridge can operate on all SR interfaces supported by the Bay Networks router *except IP*, but including

- Token Ring
- Bay Networks serial

- Frame Relay
- SMDS
- PPP
- Ethernet/802.3 encapsulation
- FDDI encapsulation
- Native SRB on FDDI

Loop-Free Operation

Loops occur in the network when there are several different routes between hosts. Bridges may forward traffic indefinitely around the loops, which results in degraded network performance. To eliminate loops, you can use one of the methods described in the following sections.

Physically Disabling Loops

You can discover loops in your network using a configuration diagram. Then you can physically adjust the network configuration to eliminate the loops. For example, assume that Figure 4-1 is a diagram of a portion of your network.

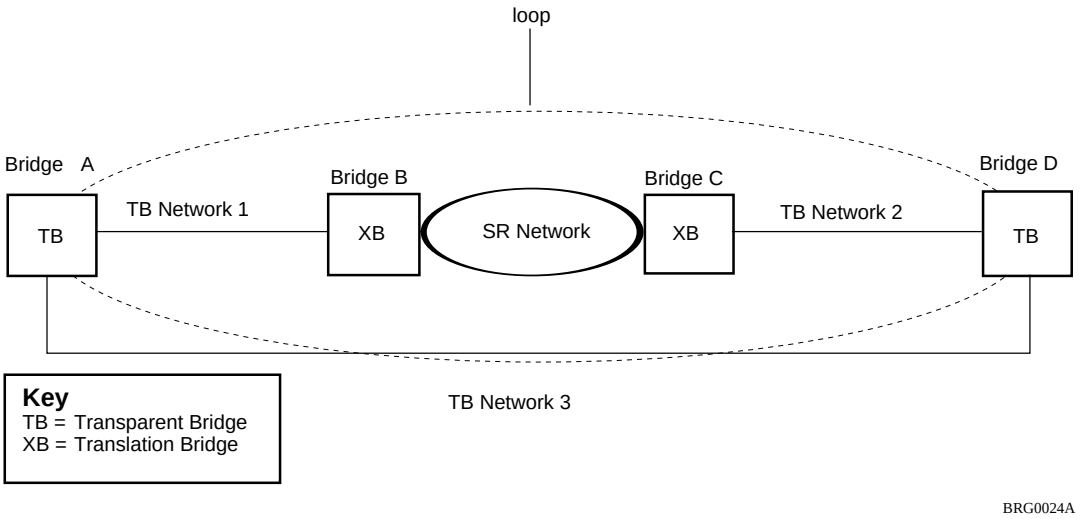


Figure 4-1. Network Configuration with Potential Loop

You want to send a packet from TB Network 1 to TB Network 2. As shown in the figure, there are two possible routes between these two networks:

- Through Bridge B, across the SR network, through Bridge C, to the destination on TB Network 2.
- Through Bridge A, across TB Network 3, through Bridge D, to the destination on TB Network 2.

To avoid continuous looping of the packet around these two paths, you can disable Bridge A or Bridge D. This eliminates the possibility of the packet using the second route. If you cannot disable a path, you can disable translation on one part of the path.

Using the Spanning Tree Protocol

A second way to eliminate loops in the network is to use the spanning tree algorithm, which discovers and eliminates redundant paths in the network topology by disabling the appropriate bridges.

You can use the spanning tree with any TB network, but only if the translation bridge uses Token Ring interfaces to the SR network. For example, you cannot use the spanning tree algorithm with translation bridging if your interface to the SR network is Ethernet, using Bay Networks SR encapsulation. Figure 4-2 shows an example of a spanning tree environment with translation bridging.

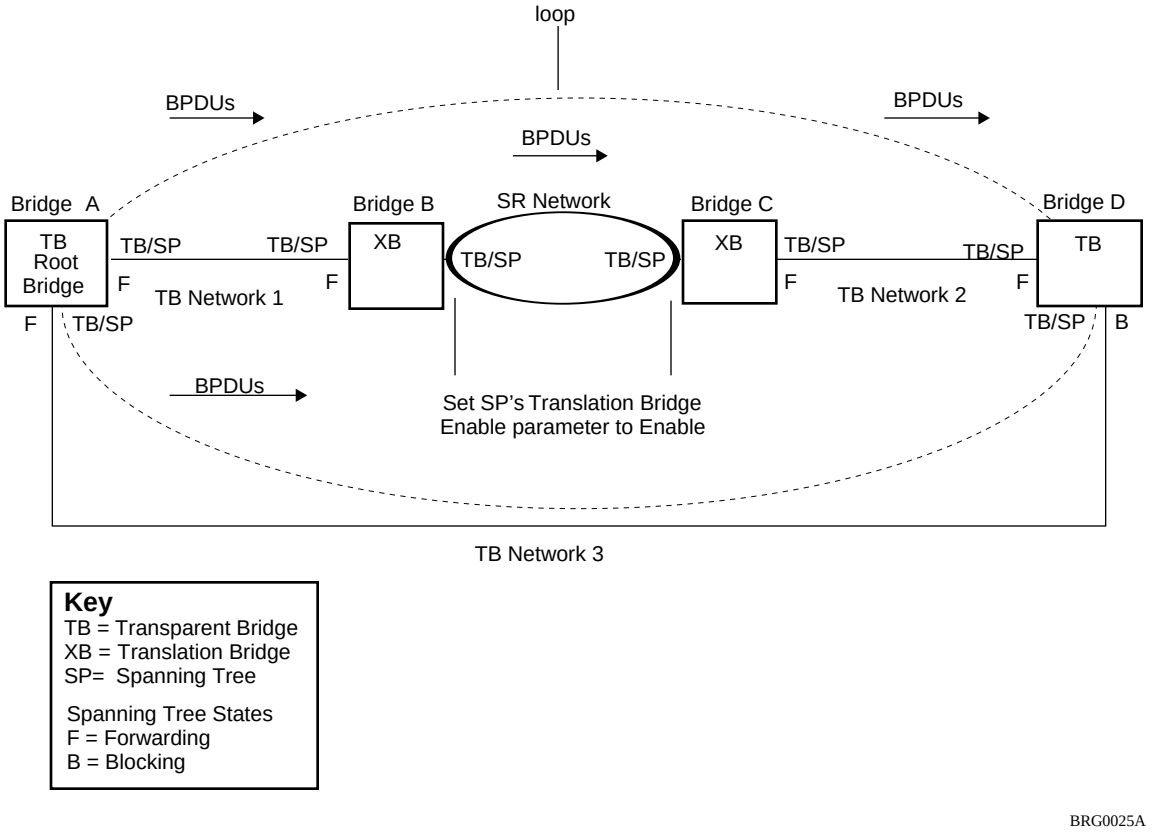


Figure 4-2. Spanning Tree with Translation Bridging

When you use the spanning tree protocol in a translation bridging environment, the token ring interfaces of the translation bridge send out special spanning tree bridge PDUs as spanning tree explorer frames (STEs). These BPDUs are essentially transparent spanning tree bridge PDUs adapted for the source route environment. These spanning tree BPDUs have no relation to whether you configured the source route bridge as a spanning tree. They are simply sent as STEs so that if a source route spanning tree exists, their impact on network traffic is minimized.

The destination MAC address for these BPDUs is the bit-swapped address used for transparent spanning tree BPDUs. This address differs from the address used for SRB spanning tree BPDUs. The transparent spanning tree then views the entire source route network as a single segment. To decide which translation bridge token ring ports should forward or block trafffic to this network segment, the router uses the normal transparent bridge spanning tree algorithm based on bridge priority, bridge MAC address, and port priority.

When designing complex translation bridge network topologies involving loops between the TB and SR networks, consider how the extended transparent-translating bridge spanning tree will converge so that you can determine which translation bridge should forward traffic to the SR network.

Procedure for Configuring the Translation Bridge on Your Network

To configure the translation bridge to work with your network:

1. **Enable the bridge on all interfaces attached to TB networks.**

   Refer to Chapter 1 for details on enabling bridging.

2. **Enable source routing on all interfaces attached to SR networks.**

   Refer to Chapter 2 for details on enabling source routing.

3. **Enable the translation bridge for each interface attached to an SR network that you want to participate in the translation bridge.**

   Refer to "Enabling Source Routing Translate/LB Service" for instructions. Use the Bridge Interfaces window to set the Translation Bridge Enable parameter to Enable. (Refer to Chapter 1 for details on configuring bridge parameters.)

4. **Create the translation bridge on the router.**

   Refer to "Creating the Translation Bridge" later in this chapter for instructions.

   Once you create the translation bridge, all TB interfaces on the router automatically participate in translation bridging.

5. **Enable the spanning tree on all TB and SR interfaces on the network on which you want to use the translation bridge if you want to use the spanning tree algorithm to eliminate loops in the network.**

Remember that the spanning tree algorithm works only if you use Token Ring interfaces to the SR network. If you use a different kind of interface to the SR network, you must use another method to eliminate loops. (Refer to the previous section, "Loop-Free Operation," for details on methods for eliminating loops.)

6. **Set the spanning tree's Translation Bridge Enable parameter to Enable for all Token Ring SR interfaces on which you enabled spanning tree.**

Enabling Source Routing Translate/LB Service

To enable Translate/LB on an interface, complete the following steps:

1. **From the Select Protocols menu, select the Translate/LB option that is directly under the Source Routing option.**

   Note that the Configuration Manager also selects the Source Routing option, because the Translate/Learning Bridge protocol cannot run without source routing enabled.

   The Edit Translation Bridge Global Parameters window appears (Figure 4-3).

2. **Configure the Virtual LAN ID parameter and click on OK.**

   Use the description that follows as a guide.

   If you have not yet enabled source routing on any circuit, the Edit Source Routing Global Parameters window appears (Figure 2-14). If you have enabled source routing on some other circuit, the SR Interface List window appears (Figure 2-15).

   Refer to "Enabling Source Routing Services on an Interface" in Chapter 2 to configure the necessary source routing parameters.

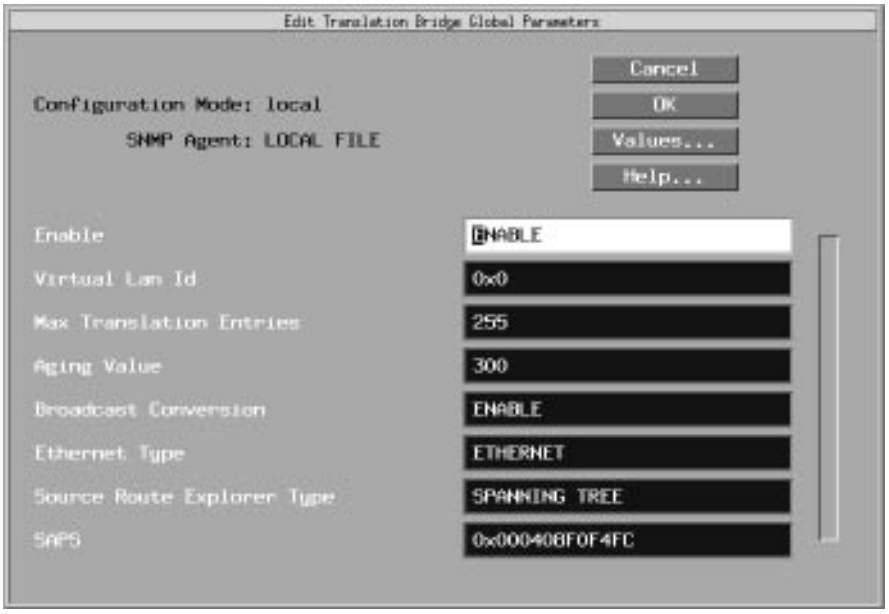


Figure 4-3. Edit Translation Bridge Global Parameters Window

Parameter: **Virtual LAN ID**

Default: 0x0

Range: 0x1 to 0xfff

Function: Assigns the transparently bridged network a ring number. To stations on the source routing network, the entire transparently bridged network appears to be one additional network segment or ring, identified by this ring number. When the SR bridge receives a frame destined for this ring number, it passes it to the translation bridge.

Instructions: Specify a ring number that is not already being used by the source routing network. The number you use should not be the same as any LAN ID, group LAN ID, or internal LAN ID number that is configured on any of the SR bridges on the network. We recommend that you configure the same ring number on all translation bridges on the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.11.3

Note: You cannot use the value 0x0 that appears initially in the Virtual LAN ID parameter box. You must specify a value for this parameter that is within the given range.

Creating the Translation Bridge

To configure the translation bridge to run on the router, select Protocols > Translation Bridge > Create TB in the Configuration Manager window (Figure 4-4).

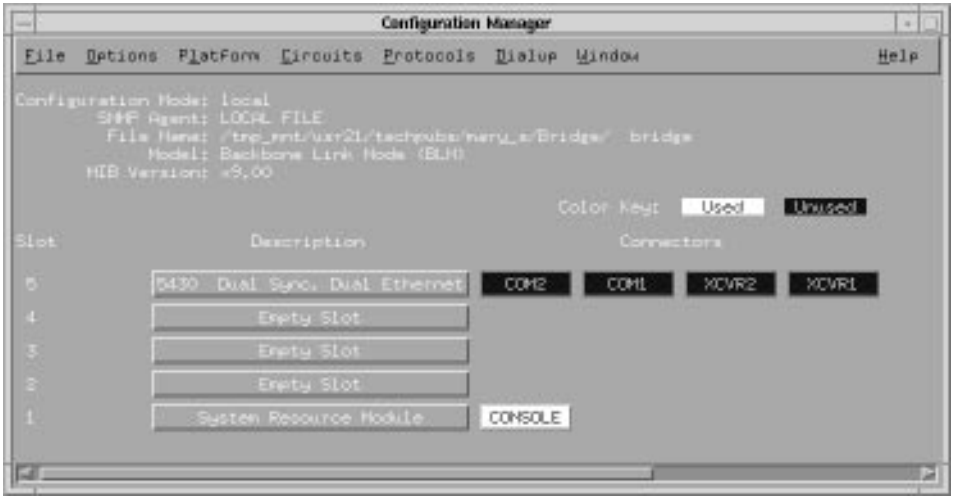


Figure 4-4. Configuration Manager Window

You can now operate the translation bridge on the router. Refer to the next section for details on optimizing translation bridge performance for your network.

Editing Translation Bridge Parameters

Once you configure the translation bridge to operate on the router, you use the Configuration Manager to edit the translation bridge parameters. This section describes how to edit the translation bridge parameters.

You access the translation bridge parameters from the Configuration Manager window (refer to Figure 4-4).

For each translation bridge parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Editing Translation Bridge Global Parameters

To edit the translation bridge global parameters:

1. **Select Protocols > Global Protocols > Translation Bridge > Global in the Configuration Manager window (refer to Figure 4-4).**

   The Edit Translation Bridge Global Parameters window appears (Figure 4-5).

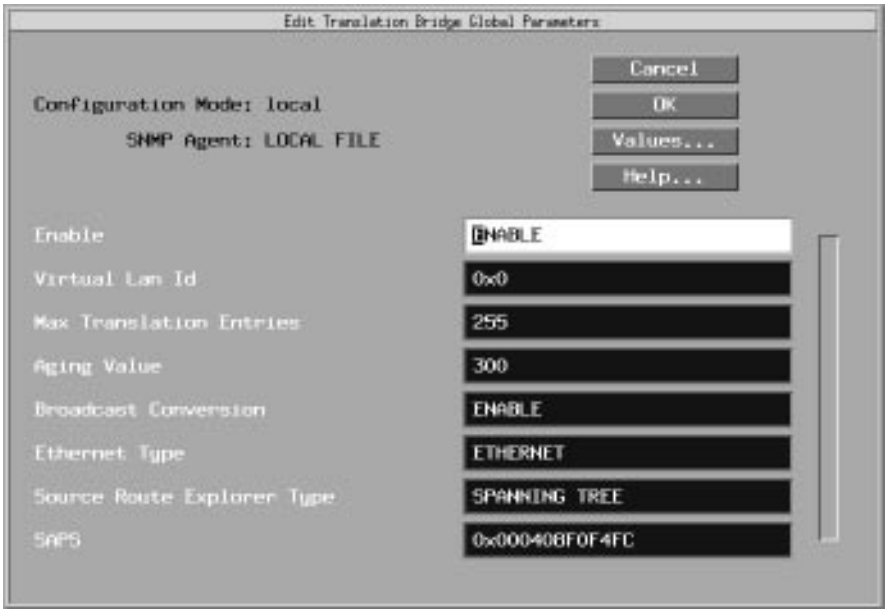


Figure 4-5. Edit Translation Bridge Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

Translation Bridge Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Translation Bridge Global Parameters window (refer to Figure 4-5).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Toggles on and off the translation bridge for the router.
Instructions:	Set to Disable to turn off translation bridging for the entire router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.2

Parameter:	**Virtual LAN ID**
Default:	0x0
Range:	0x1 to 0x0fff
Function:	Assigns the transparently bridged network a ring number. To stations on the source routing network, the entire transparently bridged network appears to be one additional network segment or ring, identified by this ring number. When the SR bridge receives a frame destined for this ring number, it passes it to the translation bridge.
Instructions:	Specify a ring number that is not already being used by the source routing network. The number you use should not be the same as any LAN ID, group LAN ID, or internal LAN ID number that is configured on any of the SR bridges on the network. We recommend that you configure the same ring number on all translation bridges on the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.3

Parameter:	**Max Translation Entries**
Default:	255
Options:	Any integer value
Function:	Specifies the maximum number of source routing addresses with routing information that the translation bridge can store in its RIF table. Ideally, this number should be equal to or greater than the number of stations on the source routed network that will communicate with stations on the transparently bridged network. If there is not enough room in the RIF table, the translation bridge does not store routing information for some stations. When the translation bridge receives traffic for those stations, it forwards the traffic as explorer frames. However, the more entries allowed in the RIF table, the more memory the translation bridges may consume. For each RIF that the translation bridge stores in the RIF table, the router creates an entry in the transparent bridge forwarding table. Increase the maximum transparent bridge forwarding table size by this value to account for addresses learned from the source route network.
Instructions:	Enter the number of addresses that the translation bridge can store in its RIF table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.4

Parameter:	**Aging Value**
Default:	300 seconds
Options:	Any integer value
Function:	Specifies how long an address entry remains in the forwarding and RIF tables when no data from that address has been received. The larger you make this value, the more time it takes the bridge to adjust to changes in the network. The smaller you make this value, the more processing the translation bridge must perform to delete and then relist infrequently used addresses.
Instructions:	Specify the number of seconds that inactive addresses should be retained.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.6

Parameter:	**Broadcast Conversion**
Default:	Enable
Options:	Enable | Disable
Function:	If you enable this feature, when the translation bridge receives a frame destined for the 802.3 broadcast address (0xFFFFFFFFFFFF), it converts the address to the 802.5 broadcast address (0xC000FFFFFFFF), and vice versa.
Instructions:	Set to Disable if you do not want the translation bridge to convert the broadcast address. When you disable this parameter, the translation bridge sends broadcast frames with the 802.3 broadcast address (0xFFFFFFFFFFFF) out the source route interfaces.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.7

Parameter:	**Ethernet Type**
Default:	Ethernet
Options:	Ethernet | IEEE8023
Function:	Specifies the default type of frame to be sent to the transparently bridged network, either Ethernet Version 2 (Ethernet) or Ethernet 802.3 (IEEE8023).
Instructions:	Specify the frame type that will be used by most of the Ethernet endstations on the network. (You can indicate specific addresses that use the other Ethernet type. Refer to "Editing Translation Bridge Station Type" later in this chapter.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.8

Parameter:	**Source Route Explorer Type**
Default:	Spanning Tree
Options:	Spanning Tree | All Routes
Function:	When the translation bridge software forwards a frame with an unknown destination address onto the source routed network, it sends the frame as either an STE (spanning tree explorer) or ARE (all-routes explorer) frame. By default, the translation bridge is configured to use STE frames, so as not to burden the source routed network with excessive ARE traffic. Using STE frames, however, forces all traffic flowing over the translation bridge to follow the spanning tree route through the network, which may not be the optimal route.
Instructions:	If you are connecting transparently bridged networks across a large source routed network, you may want to configure the translation bridge to forward frames as AREs, so that frames can follow routes other than the spanning tree route across the source routed LAN. Consider, however, that AREs may generate an unacceptable level of traffic on the larger network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.9

Parameter:	**SAPS**
Default:	000408F0F4FC
Options:	Any hexadecimal value
Function:	The translation bridge supports the transfer of LLC-based traffic, as indicated by the SAP (service access point) value. This parameter allows you to designate the SAPs that identify the protocols you want the translation bridge to accept and translate. By default, the translation bridge accepts NetBIOS, SNA, and LNM (LAN Network Manager) SAPs.
Instructions:	Specify SAPs that the translation bridge will accept.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.11.10

Editing Translation Bridge MAC Address Conversions

Token Ring networks use functional addresses for frames addressed to more than one station; Ethernet networks use multicast addresses for these frames. The Translation Bridge Address Mapping window allows you to map Token Ring functional addresses to Ethernet multicast addresses.

When the translation bridge receives a multicast frame from an Ethernet network destined for a Token Ring network, it translates the frame's multicast address to the mapped Token Ring functional address. The translation bridge converts the addresses of functional frames going from Token Ring to Ethernet to the mapped multicast address.

Note: You do not need to map functional addresses that are bit-reversed versions of the multicast addresses. The translation bridge handles these conversions automatically.

Adding an Address Mapping

To add an address mapping:

1. **Select Protocols > Global Protocols > Translation Bridge > MAC Address Conversions from the Configuration Manager window (refer to Figure 4-4).**

   The Address Mapping List window appears (Figure 4-6).

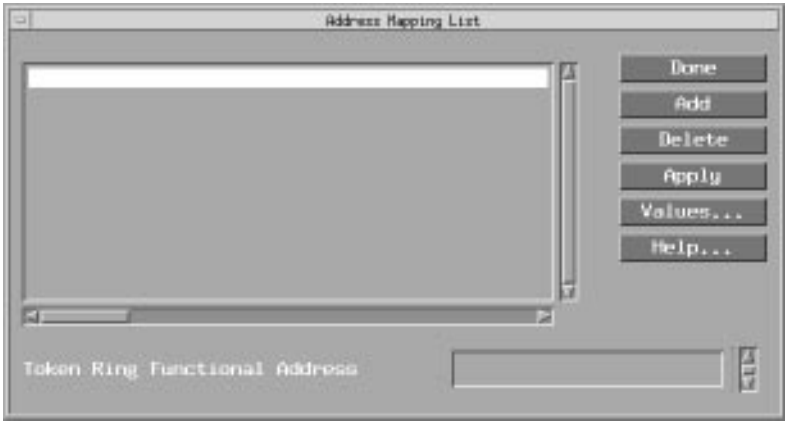


Figure 4-6. Address Mapping List Window

2. **Click on Add.**

   The Translation Bridge Address Mapping window appears (Figure 4-7).

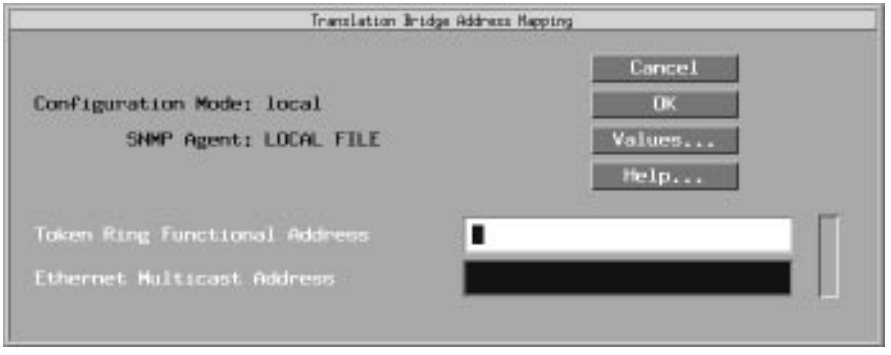


Figure 4-7. Translation Bridge Address Mapping Window

3. **Edit the parameters, using the descriptions in the next section as a guide.**
4. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Address Mapping List window.

Translation Bridge Address Mapping Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Address Mapping List and Translation Bridge Address Mapping windows (refer to Figures 4-6 and 4-7).

Parameter:	**Token Ring Functional Address**
Default:	None
Options:	Any valid functional address
Function:	Indicates the functional address of the Token Ring station.
Instructions:	Enter a valid functional address in canonical (Ethernet) format.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.12.1.3

Parameter:	**Ethernet Multicast Address**
Default:	None
Options:	Any valid Ethernet multicast address
Function:	Indicates the Ethernet multicast address.
Instructions:	Enter a valid Ethernet multicast address in canonical (Ethernet) format.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.12.1.2

Deleting an Address Mapping

To delete an address mapping:

1. **Select Protocols > Global Protocols > Translation Bridge > MAC Address Conversions from the Configuration Manager window (refer to Figure 4-4).**

   The Address Mapping List window appears (refer to Figure 4-6).

2. **Select the address you want to delete. Then click on Delete.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Editing Translation Bridge Station Type

This section describes how to configure the translation bridge so that it always translates frames destined for certain Ethernet endstations into a particular Ethernet type, regardless of how you configure the Ethernet Station Type parameter.

Adding a New Address to the Station List

To add a new address to the station list:

1. **Select Protocols > Global Protocols > Translation Bridge > Ethernet Type List from the Configuration Manager window (refer to Figure 4-4).**

   The Ethernet Station Type List window appears (Figure 4-8).

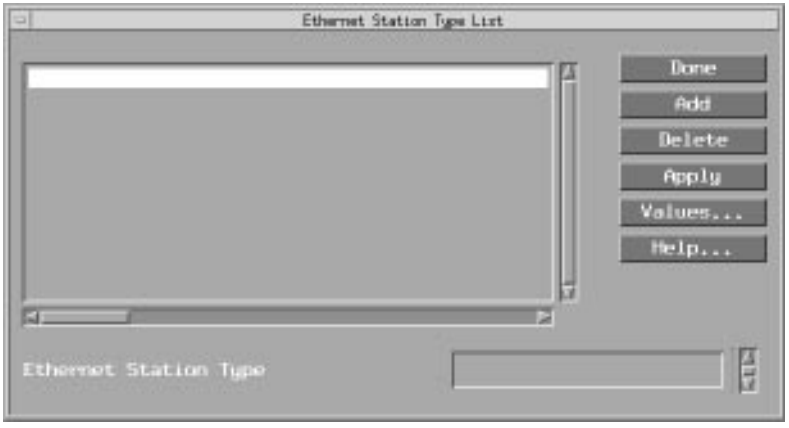


Figure 4-8. Ethernet Station Type List Window

2. **Click on Add.**

   The Translation Bridge Address Mapping window appears (Figure 4-9).

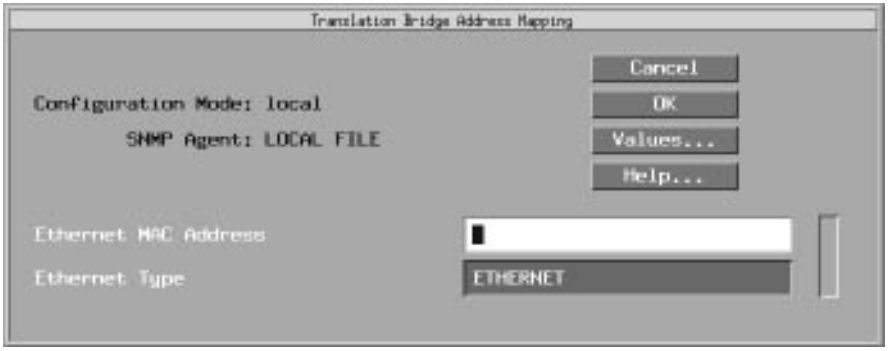


Figure 4-9. Translation Bridge Address Mapping Window

3. **Edit the parameters, using the descriptions in the next section as a guide.**
4. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Ethernet Station Type List window.
5. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Translation Bridge Ethernet Address Mapping Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Translation Bridge Address Mapping window (refer to Figure 4-9).

Parameter:	**Ethernet MAC Address**
Default:	None
Options:	Any valid Ethernet MAC address
Function:	Indicates the address of the station whose type you want to specify.
Instructions:	Enter the Ethernet MAC address of the desired station.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.14.1.2

Parameter:	**Ethernet Type**
Default:	Ethernet
Options:	Ethernet | IEEE8023
Function:	Specifies the type of frame you want to use for this station, either Ethernet Version 2 (Ethernet) or Ethernet 802.3 (IEEE8023).
Instructions:	Select the type you want to use for this station.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.2.14.1.3

Deleting a Station

To delete a station from the station list:

1. **Select Protocols > Global Protocols > Translation Bridge > Ethernet Type List from the Configuration Manager window (refer to Figure 4-4).**

   The Ethernet Station Type List window appears (refer to Figure 4-8).

2. **Select the address you want to delete. Then click on Delete.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the window.**

   Site Manager returns you to the Configuration Manager window.

Deleting the Translation Bridge from the Router

To delete the translation bridge from the router, select Protocols > Global Protocols > Translation Bridge > Delete TB from the Configuration Manager window (refer to Figure 4-4).

The translation bridge is no longer enabled on the router.

Chapter 5
Using Native Mode LAN Services

This chapter provides an overview of Native Mode LAN (NML) services and implementation notes about using NML services. It also describes how to use Site Manager to

- Create an NML port
- Edit NML interface parameters
- Assign an access list to a port

Native Mode LAN Overview

Native Mode LAN services allow you to define closed user groups within a shared bridging environment.

Each NML closed user group consists of multiple LANs and is identified by a closed user group ID (CUGID). You assign the CUGID to each port that supports a LAN belonging to the closed user group and provide each port with an access list that contains the CUGID. A CUGID is a value in the range of $0\text{-}2^{31}$.

You select a single CUGID for the group and assign the value to each NML-configured port that provides a bridge connection for a LAN in the group. You can also create a range of CUGIDs for the group and assign a different CUGID to each port.

The shared network in Figure 5-1 includes two closed user groups: Star and Moon. Closed User Group Star consists of two local area networks: LAN A on the West Side and LAN C on the East Side. Closed User Group Moon contains three local area networks distributed between the East Side and the West Side: LAN B, LAN D, and LAN E.

Each LAN in a closed user group is connected to a bridge through an NML port. LAN A in the Star Closed User Group, for example, connects to Bridge 1 on NML Port 1. LAN C connects to Bridge 2 through NML Port 6.

NML Port 1 and NML Port 6 are assigned the Star CUGID. They are also provided with an access list that contains the Star CUGID.

An NML port adds its CUGID to each frame that enters the bridge from a closed user group and uses its access list to validate the CUGID on each frame that attempts to exit the bridge through the port. In this way, traffic on the LANs within a closed user group is restricted to frames that bear the group's CUGID.

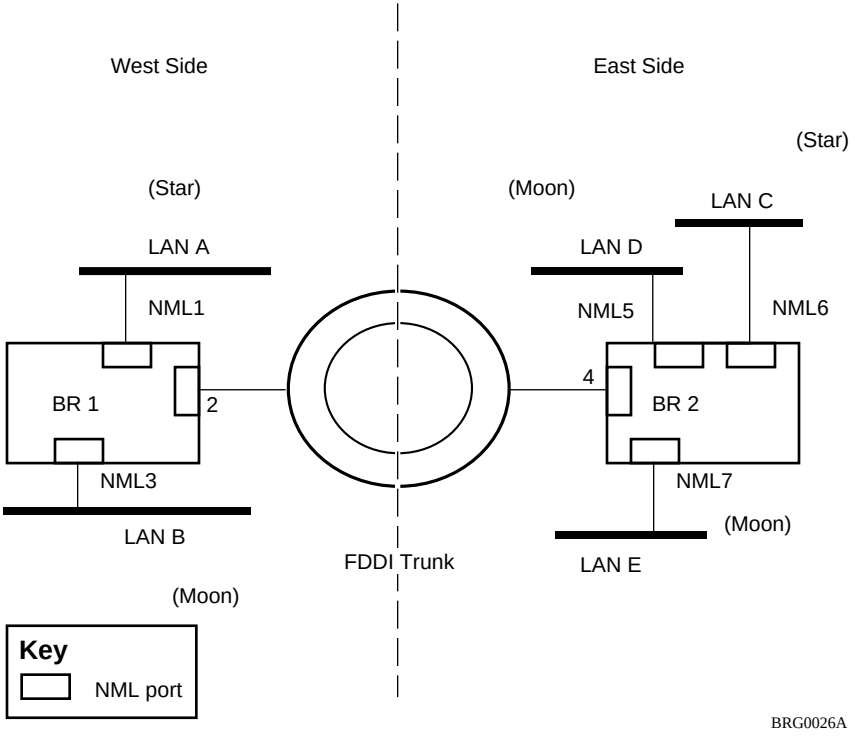


Figure 5-1. NML Closed User Groups

In Figure 5-1, for example, consider what happens when a member of the Star Closed User Group on LAN A sends a frame to another member of the Star group located on LAN C.

1. **The frame, properly addressed, enters Bridge 1 through NML Port 1.**
2. **Port 1 labels the frame with the Star CUGID.**
3. **Bridge 1 forwards the frame to Bridge 2 over the FDDI trunk.**
4. **The frame attempts to exit Bridge 2 through Port 6. Port 6 examines the CUGID on the frame.**

   The CUGID on the frame matches the CUGID on the port's access list. Port 6 forwards the frame to LAN C in the Star Closed User Group.

Defining a Closed User Group

To define a closed user group:

1. **Select a CUGID for the closed user group.**
2. **Create an NML port for each LAN in the closed user group by adding the NML protocol to an existing bridge circuit.**

   Refer to Chapter 2 of *Configuring Routers* for details.

3. **Assign the group CUGID to each port and specify other NML port parameters.**

   Refer to "NML Add Security Range Parameters" later in this chapter for details.

4. **Provide each NML port with an access list containing the group CUGID.**

   Refer to "Assigning an Access List to a Port" later in this chapter for details.

Implementation Notes

The following sections describe some Native Mode LAN configuration features.

Defining a Closed User Group That Permits Overlapping Network Traffic

In an NML environment, overlapping traffic occurs when members of one closed group are allowed to exchange information with users on some, but not all, LANs of another closed group.

To permit overlapping traffic on a LAN that is part of a closed user group, you assign an access list to the LAN's NML port that contains the CUGID for all groups that are allowed access to the LAN. This requires the use of unique CUGIDs for each involved port.

For example, members of the Star group need to exchange information with Moon group members on LAN E (refer to Figure 5-1). To define LAN E as a LAN that permits overlapping traffic, you assign NML Port 7 an access list that includes both Moon CUGIDs and Star CUGIDs.

Controlling NML Traffic on a Network Trunk

Network trunks carry the frames of all closed user groups. In Figure 5-1, for example, the FDDI link between Bridge 1 and Bridge 2 is a network trunk. The NML service allows you to control traffic on a trunk by blocking access to the trunk by frames that originate from LANs that you specify. If you determine, for example, that frames originating from a LAN that is part of a given closed user group can never reach their destination via the trunk, you can block the frames from traveling on the trunk. This feature helps reduce network traffic on the trunk by eliminating useless frames.

For example, the Moon closed user group in Figure 5-1 closes its office on the West Side, dismantling LAN B and NML Port 3. To ensure that no frames destined for Port 3 get onto the FDDI trunk (needlessly increasing the traffic load), you create an NML trunk port, Port 4, and provide it with an access list that contains the CUGIDs of the remaining Moon ports. The NML port checks the CUGID of all frames that attempt to exit from the bridge onto the trunk and drops all frames containing a Moon CUGID.

Caution: We strongly recommend that you avoid using this feature in conjunction with the spanning tree algorithm.

Enabling NML Services

Complete the following steps to enable NML on an interface:

1. **Select Native Mode LAN from the Select Protocols window.**

   The Select Protocol window appears after you either select a link or net module connector, or finish configuring a WAN circuit. Note that when you select Native Mode LAN from the menu, Configuration Manager automatically selects the Bridge protocol.

2. **Click on OK.**

   The Configuration Manager displays a window with the message

   ```
   Do you want to edit the NML interface details?
   ```

3. **Click on OK.**

   The Configuration Manager displays the Edit NML Interface window (Figure 5-2).

Figure 5-2. Edit NML Interface Window

4. **For instructions on editing NML parameters and assigning an access list to a port, refer to "Editing NML Interface Parameters" and "Assigning an Access List to a Port" later in this chapter.**

Editing NML Parameters

Once you configure a circuit to support NML, you can use the Configuration Manager to edit the NML parameters. This section describes how to edit these parameters.

Note: The instructions in this section assume that you already configured NML on the router. If you did not, refer to Configuring Routers for details.

For each NML parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

You access all NML parameters from the Configuration Manager window (Figure 5-3). Refer to *Configuring Routers* for details on accessing this window.

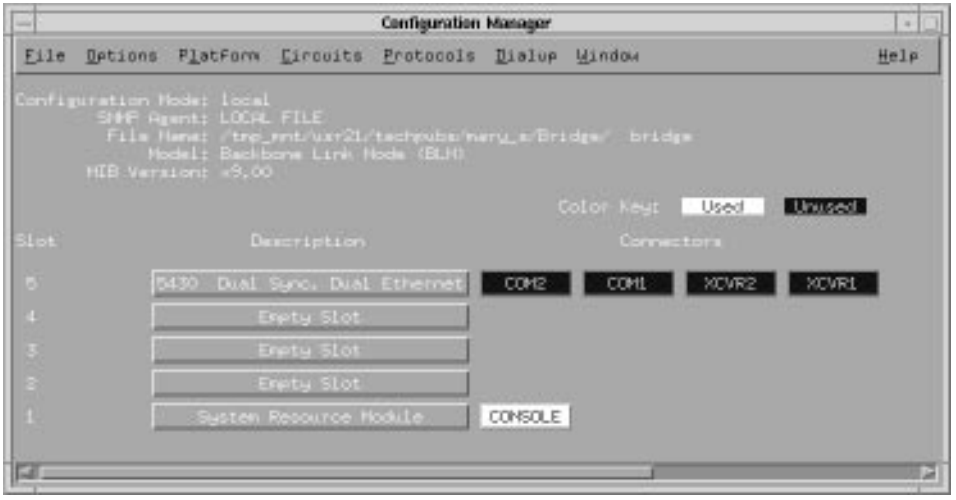


Figure 5-3. Configuration Manager Window

Editing NML Interface Parameters

To edit NML interface parameters:

1. **Select Protocols > NML > Interfaces from the Configuration Manager window (refer to Figure 5-3).**

   The NML Interfaces window appears (Figure 5-4).

Figure 5-4. NML Interfaces Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   Site Manager returns you to the Configuration Manager window.

NML Interface Parameter Descriptions

Use the following descriptions as a guide when you configure the parameters in the NML Interfaces window (refer to Figure 5-4).

Parameter:	**Disable**
Default:	Enabled
Options:	Enabled | Disabled
Function:	Enables and disables the NML service on this circuit.
Instructions:	Set to Disabled if you want to temporarily disable NML on this circuit rather than delete it. Set to Enabled if you previously disabled NML but now want to re-enable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.2

Parameter:	**Add Security Header**
Default:	Add Security
Options:	No Security | Add Security | Check Security
Function:	Specifies whether the NML port adds a CUGID to frames entering the bridge and performs an access check on frames that exit the bridge. Add Security --The NML port adds a CUGID to every frame that enters the bridge on the circuit and performs an access check on every frame that attempts to exit from the bridge on the circuit. Depending on the option you specify for the Security List Action parameter, the NML port forwards or drops the exiting frame. In forwarding a frame, the NML port strips off the CUGID. Check Security -- The NML port performs an access check on each frame that attempts to exit from the bridge on the circuit. Depending on the option you specify for the Security List Action parameter, the NML port forwards or drops the exiting frame. The NML port forwards the frame with the CUGID in place. It does not strip off the identifier. No Security -- The port performs no access validation.
Instructions:	Specify Add Security for a circuit that provides a bridge connection for a LAN belonging to a closed user group. Specify Check Security for a circuit that provides a bridge connection for a network trunk. For information about NML services for network trunks, refer to "Controlling NML Traffic on a Network Trunk."
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.4

Parameter:	**SAID Type**
Default:	Individual
Options:	Individual | Group
Function:	Ignored by Bay Networks. Supplied for 802.10 interoperability.
Instructions:	Accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.5

Parameter:	**SAID Value**
Default:	0
Range:	0 to 2^{31} (2,147,483,648)
Function:	Ignored by Bay Networks. Supplied for 802.10 interoperability.
Instructions:	Accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.6

Parameter:	**CUG Value**
Default:	0
Options:	A decimal value or a set of values in the range 0 to 2^{31} (2,147,483,648)
Function:	Specifies the CUGID that you assign to the circuit.
Instructions:	In most cases, you create a single CUGID for the closed user group and assign the value to each circuit that supports the group. If you need to specify different access requirements for certain LANs in the closed user group, create a range of CUGIDs and assign a different one to each LAN.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.7

Parameter:	**Security List Action**
Default:	Forward
Options:	Drop | Forward
Function:	Specifies whether the NML port forwards or drops a frame when it finds a match on the access list.
Instructions:	If the access list is an inclusive CUGID list, specify Forward. The port forwards to the attached LAN all frames labeled with the CUGID. If the list is an exclusive list, specify Drop. The port drops all frames labeled with the CUGID.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.1.5.2.1.8

Assigning an Access List to a Port

To validate a frame that is attempting to exit through an NML port, the port consults an access list. If the CUGID on the frame matches a CUGID on the list, the port takes the action you have specified: forwarding the frame and discarding the CUGID, forwarding the frame and retaining the CUGID, or dropping the frame.

You create an inclusive list or an exclusive list for each NML port that supports the closed user group. When the port finds a match on an inclusive list, it forwards the frame. When the NML port finds a match on an exclusive list, it drops the frame.

To assign an access list to a port so that you can specify a start and end range of CUGIDs for the circuit on which the port is located:

1. **Select Protocols > NML > Interfaces from the Configuration Manager window (refer to Figure 5-3).**

   The NML Interfaces window appears (refer to Figure 5-4).

2. **Click on Security List.**

   The NML Filters window appears (Figure 5-5).

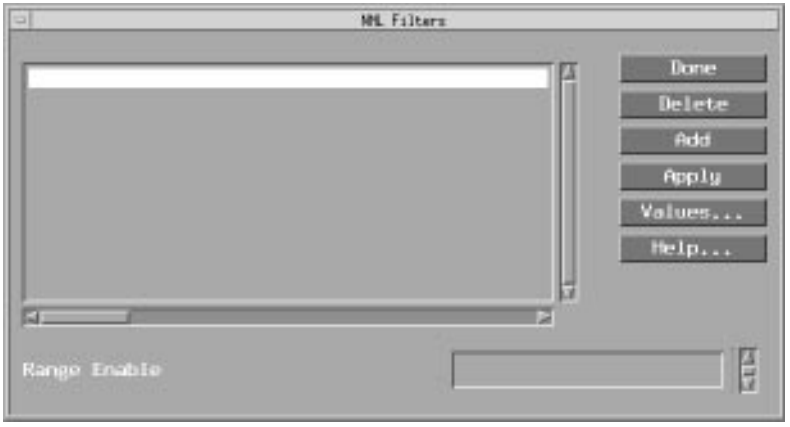


Figure 5-5. NML Filters Window

3. **Select the circuit to which you want to add an access list.**
4. **Click on Add to add a security range.**

   The NML Add Security Range window appears (Figure 5-6).

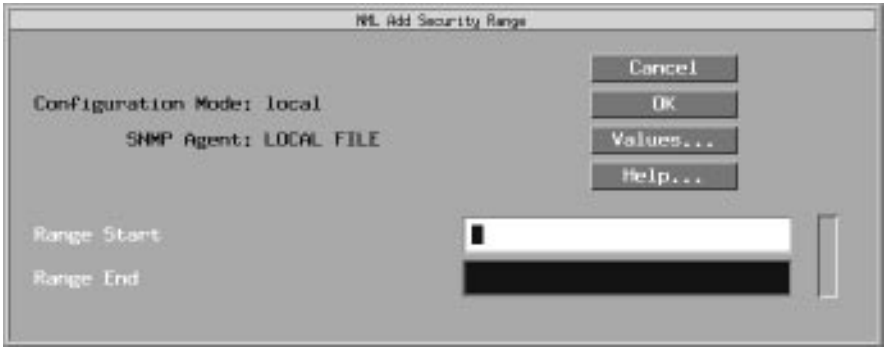


Figure 5-6. NML Add Security Range Window

5. **Specify a CUGID or a range of CUGIDs, using the parameter descriptions in the next section as a guide.**
6. **Click on OK.**

Site Manager returns you to the NML Filters window.

7. **Repeat Steps 3 through 6 to add additional start and end ranges.**
8. **Click on Apply to save your changes.**

   Site Manager returns you to the NML Interfaces window.

NML Add Security Range Parameters

Use these parameter descriptions as a guide when you add security ranges for a selected circuit in the NML Add Security Range window (refer to Figure 5-6).

Note: To specify only one CUGID, enter the same value in both the Range Start and Range End parameters.

Parameter:	**Range Start**
Default:	None
Range:	0 to 2^{31} (2,147,483,648)
Function:	Indicates the start of the CUGID range.
Instructions:	Enter a value between 0 and 2^{31}.
MIB Object ID:	None

Parameter:	**Range End**
Default:	None
Range:	0 to 2^{31} (2,147,483,648)
Function:	Indicates the end of the CUGID range.
Instructions:	Enter a value between 0 and 2^{31}.
MIB Object ID:	None

Enabling Ranges

To enable or disable the ranges you set for a selected circuit:

1. **Select the Circuits > Edit Circuits option in the Configuration Manager window (refer to Figure 5-3).**

   The Circuit List window appears (Figure 5-7).

Figure 5-7. Circuit List Window

2. **Select the circuit whose access list you want to view.**
3. **Click on Edit.**

   The Circuit Definition window appears, with the circuit you selected highlighted (Figure 5-8).

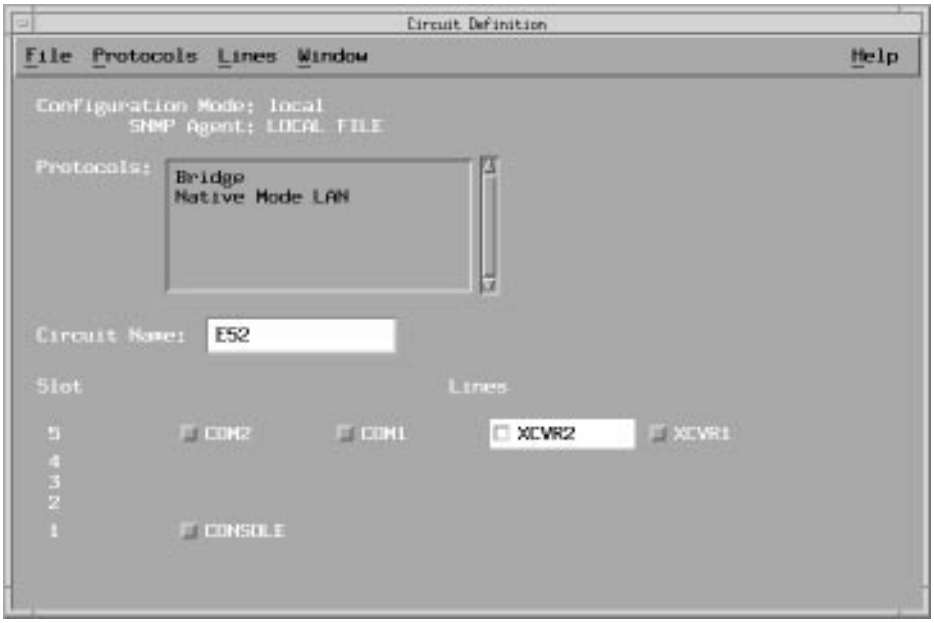


Figure 5-8. Circuit Definition Window

4. **Select Protocol > Edit NML > Security List.**

   The NML Filters window appears (refer to Figure 5-5).

5. **Set the Range Enable parameter to Enable or Disable, depending on whether you want the ranges you set for the specified circuit enabled or disabled.**

   Use the parameter description in the next section as a guide.

6. **Click on Done to save your changes and exit the window.**

Note: You cannot enable or disable specific ranges in a circuit.

NML Range Enable Parameter Description

Use this parameter description as a guide when you enable or disable ranges for a selected circuit in the NML Filters window (refer to Figure 5-5).

Parameter:	**Range Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Indicates whether you want the CUGID ranges you specified enabled or disabled.
Instructions:	Accept the default, Enable, or specify Disable.
MIB Object ID:	None

Deleting NML from the Router

To delete NML from the router:

1. **Select Protocols > NML > Delete NML from the Configuration Manager window (refer to Figure 5-3).**

   A message appears that prompts

   ```
   Do you REALLY want to delete NML?
   ```

2. **Click on OK.**

   You are returned to the Configuration Manager window. NML is no longer configured on the router.

Appendix A
Site Manager Default Settings

This appendix describes the Site Manager default parameter settings for the transparent bridge (including spanning tree), the source routing bridge, source routing NetBIOS broadcast reduction, the translation bridge, and Native Mode LAN services.

Table A-1. Transparent Bridge Global Parameters

Parameter	Default
Enable	Enable
Bridge Table Size	1024 entries
Enable Forwarding DB	Enable

Table A-2. Transparent Bridge Interface Parameters

Parameter	Default
Enable	If you added bridging using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable bridging on this circuit, the parameter defaults to Disable.
Translational Bridge Enable	Disable

Table A-3. Spanning Tree Global Parameters

Parameter	Default
Enable	Enable
Bridge Priority	128
Bridge MAC Address	Autoconfigured
Max Age	20 s (expressed in hundredths of a second: 2000)
Hello Time	2 s (expressed in hundredths of a second: 200)
Forward Delay	15 s (expressed in hundredths of a second: 1500)

Table A-4. Spanning Tree Interface Parameters

Parameter	Default
Enable	If you added spanning tree using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable.
Priority	128
Path Cost	1

Table A-5. Source Routing Global Parameters

Parameter	Default
Enable	Enable
SR Bridge Internal LAN ID	0x0
SR Bridge ID	0x0
SR Bridge Group LAN ID	0xfff
IP Encapsulation	Disable
Conn. IP NTWK Ring number	0x0
IP MTU Size (bytes)	4562
NetBIOS Server Name Cache	Disable
NetBIOS Client Name Cache	Disable
NetBIOS Datagram RIF Cache	Disable
15-Character NetBIOS Name Caching	Disable
Create MIB Instance for Cached Name	Enable
Max Name Cache Entries	100
Name Cache Age (secs)	300 s
Hash Entry Count	253
NetBIOS Query Cache	Disable
Create MIB Instances for Cached Query	Enable
Max Number Query Cache Entries	100
NetBIOS Query Cache Age (secs)	15 s

Table A-6. Source Routing Interface Parameters

Parameter	Default
Enable	Enable
Max number of RDs	7
Source Routing Ring Number	0x0
Outbound STEs	Accept
Inbound STEs	Accept
Frames with IP Ring	Accept
IP Address	None
NetBIOS Server Name Cache	Enable
NetBIOS Client Name Cache	Enable
NetBIOS Datagram RIF Cache	Enable
NetBIOS Query Cache	Enable
WAN Broadcast Address	-1
Encapsulation Format	Proprietary

Table A-7. Source Routing Bridge ID Parameter

Parameter	Default
New Source Routing Bridge ID	None

Table A-8. IP Explorer Address Parameter

Parameter	Default
New SR Bridge Explorer IP address	None

Table A-9. Source Route Spanning Tree Global Parameters

Parameter	Default
Spanning Tree Enable	Enable
Bridge Priority	128
Bridge MAC Address	Autoconfigured
Max Age	20 s
Hello Time	2 s
Forward Delay	15 s

Table A-10. Source Route Spanning Tree Interface Parameters

Parameter	Default
Spanning Tree Enable	If you added spanning tree using either the Quick-Start procedure or the configuring-circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable.
Path Cost	1

Table A-11. NetBIOS Global Parameters

Parameter	Default
NetBIOS Server Name Cache	Disable
NetBIOS Client Name Cache	Disable
NetBIOS Datagram RIF Cache	Disable
15-Character NetBIOS Name Caching	Disable
Create MIB Instances for Cached Name	Enable
Max Name Cache Entries	100 s
Name Cache Age (secs)	300 s
Hash Entry Count	253
NetBIOS Query Cache	Disable
Create MIB Instances for Cached Query	Enable
Max Number Query Cache Entries	100
NetBIOS Query Cache Age (secs)	15 s

Table A-12. NetBIOS Interface Parameters

Parameter	Default
NetBIOS Server Name Cache	Enable
NetBIOS Client Name Cache	Enable
NetBIOS Datagram RIF Cache	Enable
NetBIOS Query Cache	Enable

Table A-13. NetBIOS Static Name Parameters

Parameter	Default
Enable	Enable
NetBIOS Station Name	None
Mac Address	None
RIF from Router	None

Table A-14. Translation Bridge Global Parameters

Parameter	Default
Enable	Enable
Virtual Lan ID	0x0
Max Translation Entries	255
Aging Value	300 s
Broadcast Conversion	Enable
Ethernet Type	Ethernet
Source Route Explorer Type	Spanning Tree
SAPs	000408F0F4FC

Table A-15. Translation Bridge Address Mapping Parameters

Parameter	Default
Token Ring Functional Address	None
Ethernet Multicast Address	None

Table A-16. Translation Bridge Ethernet Address Mapping Parameters

Parameter	Default
Ethernet MAC Address	None
Ethernet Type	Ethernet

Table A-17. NML Interface Parameters

Parameter	Default
Disable	Enabled
Add Security Header	Add Security
SAID Type	Individual
SAID Value	0
CUG Value	0
Security List Action	Forward

Table A-18. NML Add Security Range Parameters

Parameter	Default
Range Start	None
Range End	None

Table A-19. NML Range Enable Parameters

Parameter	Default
Range Enable	Enable

Appendix B
Components of a Source Route Frame

A source route frame consists of the fields shown in Figure B-1.

8.02 Physical Header	Routing Info Field (RIF)	802.5 Physical Header	Data	802.5 Trailer

Figure B-1. Fields in a Source Route Frame

802.5 Physical Header

The 802.5 physical header consists of the following fields:

- Starting delimiter
- Access control field
- Frame control field
- Destination address
- Source address field

If the first (left-most) bit of the source address is 0, the frame contains no source routing information. If the first bit is a 1, the bridge code examines the frame and looks for a RIF field.

Routing Information Field (RIF)

For source routing purposes, the most important part of a frame is the Routing Information Field (RIF). This field contains the routing information needed by the bridge to forward a frame.

The RIF is an optional field. The router uses the RIF only if the frame destination is another ring. When used, the RIF is placed at the beginning of a frame's data field.

The RIF has two sections: Routing Control fields and Routing Designators (Figure B-2).

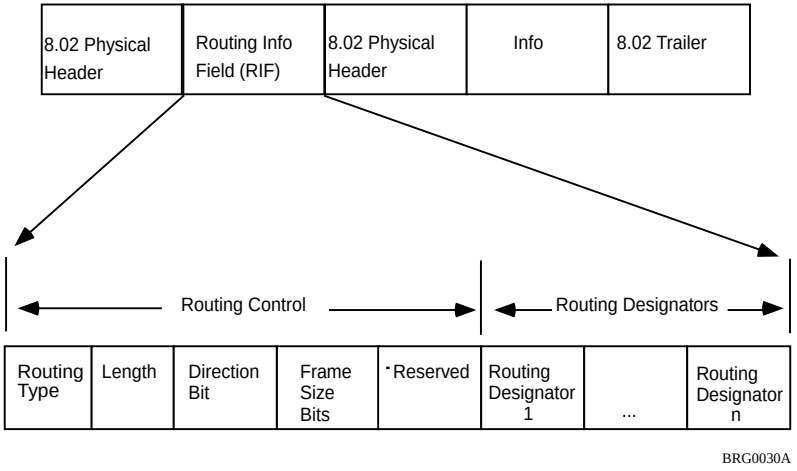


Figure B-2. Components of the RIF

Routing Control

Routing control is 2 bytes long and comprises the following bit fields:

- Routing type
- Length
- Direction bit
- Frame Size bits
- Reserved

Type of Frame

The first three bits specify the type of frame and the return frame requested. These bits take the following format:

- 0xx specifies a specifically routed frame (SRF)
- 10x specifies an all routes explorer (ARE) frame
- 11x specifies a single routes broadcast (SRB) frame

Length

The next five bits are the length of the RIF field in the frame. A source routed frame is at least two bytes in length and is called the routing control field.

Direction Bit

The direction bit determines whether the RIF is read from right to left or from left to right. As an ARE traverses the network, bit 3 is set to 0 to signify that the RIF is read from left to right. A station replying to an ARE caches the RIF field and sets the direction bit to 1 so that the RIF is read from right to left.

Frame Size Bits

As an ARE or STE traverses the network, each device that it passes through sets these bits to the largest frame size possible (in bytes). The Bay Networks router can accommodate a source route frame size up to up to a 4472 bytes over any media. The initial value of the bit string is 111 (Table B-1).

Table B-1. Frame Size Bits

Bit Pattern	Max Number of Bytes
011	1500
010	2052
011	4472
100	8144
101	11,407
110	17,800
111	Initial Value

A possible value for the routing control field follows:

011:1500010:2052011:4472100:8144101:11407110:17800

Routing Designators

The routing designator field is 2 bytes long and comprises a Ring ID and a Bridge ID. The Ring ID has 12 bits (001 through FFF) and the Bridge ID has four bits (1 through F).

When a router receives a frame such as an ARE and forwards it out an interface, the last Bridge ID is set to 0 because the router does not know the ID of the next bridge to pick up the frame.

The maximum number of routing designators in the RIF field is seven Ring ID/ Bridge ID pairs.

Index

Symbols

15-character Name Caching parameter, 3-15

802.3 frames
- translated by translation bridge, 4-6
- translated by transparent bridge, 1-3 to 1-8

A

Access list, assigning to a port, 5-11 to 5-13

Add name query frame, 3-2

Add Security Header (NML interface) parameter, 5-9

Address
- accessing, 1-22
- functional, 4-21
- maximum number allowed in forwarding table, 1-21
- multicast, 4-21
- *See also* MAC address

Aging
- names in cache, 3-8, 3-16
- translation bridge database entries, 4-2

Aging Value parameter, 4-18

All-paths broadcast routing, 2-2

All-paths explorer (APE) frame, 2-2, 4-5

All-routes explorer (ARE) frame, 2-2, 4-5

APE frames, 2-2

ARE frames, 2-2, 4-3

B

Bay Networks
- CompuServe forum, xxiv
- Customer Service FTP, xxiii
- home page on World Wide Web, xxiii
- InfoFACTS service, xxv
- publications, ordering, xx
- support programs, xxii
- Support Source CD, xxiv
- Technical Response Center, xxi, xxv
- technical support, xxi

BPDU. *See* Bridge Protocol Data Unit

Bridge (Translation). *See* Translation bridge, A-7

Bridge (transparent) global parameters
- defaults, A-1
- editing, 1-19 to 1-22

Bridge (transparent) interface parameters
- defaults, A-1
- editing, 1-22 to 1-24

Bridge (Transparent). *See* Transparent bridge

Bridge ID
- adding, 2-45, 2-47
- assigning, 2-22 to 2-23, 2-36
- deleting, 2-45 to 2-47
- of a source routing bridge, 2-2
- on ARE frame, 2-2
- with IP encapsulation, 2-5

Bridge Priority parameter, 1-26, 2-32

Bridge Protocol Data Unit (BPDU), 1-10, 1-27, 1-28, 2-53, 2-54

Bridge station type, 4-24 to 4-26

Bridge Table Size global parameter, 1-21

Bridge Tunnel Service, 1-4
Bridge, transparent. *See* Transparent bridge
Broadcast Conversion parameter, 4-19
Broadcast reduction, 3-4 to 3-9

C

Caching
  aging process, 3-8, 3-16
  client, 3-5, 3-14, 3-21
  datagram RIF, 3-6, 3-15
  disabling, 3-14
  enabling, 3-14
  lookup, 3-8
  maximum entries allowed for, 3-16
  NetBIOS names, 3-27
  query, 3-7
  server name, 3-6
  using 15 characters, 3-15
Caching NetBIOS names
  enabling, 3-27
Client name caching, 3-5, 3-14, 3-21
Closed user group (CUG)
  defining, 5-3
  ID for, 5-1
  permitting overlapping traffic using, 5-4
CompuServe, Bay Networks forum on, xxiv
Conn. IP NTWK Ring Number parameter, 2-37
Create MIB Instances for Cached Name parameter, 3-15
Create MIB Instances for Cached Query parameter, 3-18
CUG Value (NML interface) parameter, 5-10
CUGID (closed user group ID), 5-1
Customer Service FTP, xxiii
customer support. *See* getting help

D

Data link connection identifier (DLCI), 2-43
Data link switching used with NetBIOS, 3-10
Datagram, in NetBIOS, 3-4
Defaults
  IP explorer address parameters, A-4
  NetBIOS parameters, A-6
  NML parameters, A-8
  source routing parameters, A-4
  spanning tree parameters, A-2
  translation bridge parameters, A-7
  transparent bridge parameters, A-1
Disable (NML interface) parameter, 5-9
DLCI, 2-43
DLSw, used with NetBIOS, 3-10

E

Enable Forwarding DB global parameter, 1-22
Enable parameter
  bridge global, 1-20
  bridge interface, 1-24
  NetBIOS static list, 3-27
  source routing global, 2-35
  source routing interface, 2-40
  spanning tree global, 1-25
  spanning tree interface, 1-31
  translation bridge global, 4-17
Encapsulation Format parameter, 2-44
Endstation support
  in source routing, 2-9 to 2-10
Endstations
  on a source routing network, 2-2 to 2-4
Ethernet frames
  translated by translation bridge, 4-6
  translated by transparent bridge, 1-3 to 1-8
Ethernet MAC Address parameter, 4-25
Ethernet Multicast Address parameter, 4-23
Ethernet Type parameter, 4-19, 4-26
Explorer frames, used with translation bridge, 4-3 to 4-4
Explorer frames. *See* Source routing

F

FDDI frames
translated by transparent bridge, 1-3 to 1-8
Filters, 1-14
Forward Delay parameter, 1-29, 2-55
Forwarding table
bridge actions based on entries in, 1-3
flushing, 1-32
maximum number of entries allowed in, 1-21
part of learning process, 1-2
translation bridge, 4-2
Frame formats, with translation bridge, 4-6
Frame lengths, with translation bridge, 4-6
Frames with IP Ring parameter, 2-42
Functional addresses, 4-21

G

getting help
from a Bay Networks Technical Response Center, xxv
from the Support Source CD, xxiv
through CompuServe, xxiv
through Customer Service FTP, xxiii
through InfoFACTS service, xxv
through World Wide Web, xxiii
Global parameters
NetBIOS, editing, 3-13 to 3-19
source routing, editing, 2-33 to 2-38
spanning tree, editing, 1-24 to 1-29
translation bridge, editing, 4-15 to 4-20
transparent bridge, editing, 1-19 to 1-22
Group LAN ID, 2-2, 2-24, 2-36, 2-41

H

Hash Entry Count parameter, 3-17
Hello Time parameter, 1-28, 2-54

I

Inbound STEs parameter, 2-42
InfoFACTS service, xxv
Interface parameters
bridge, editing, 1-22 to 1-24
NetBIOS, editing, 3-20 to 3-22
source routing bridge, editing, 2-38 to 2-43
spanning tree, editing, 1-29 to 1-32
Interfaces, translation bridge support, 4-7
Internal LAN ID, 2-2, 2-24, 2-35, 2-41
IP Address Explorer list, 2-47 to 2-49
IP Address parameter, 2-43
IP encapsulation, 2-4 to 2-8, 2-24 to 2-25, 2-37, 2-42, 2-43
IP Encapsulation parameter, 2-37
IP Net MTU parameter, 2-38

L

LAN speeds, with translation bridge, 4-7
Lengths of frames, with translation bridge, 4-6
Loop-free topology, 4-8
See also Spanning tree algorithm

M

MAC address
accessing, 1-22
conversions by translation bridge, 4-21 to 4-23
formats with translation bridge, 4-6
maximum number allowed in forwarding table, 1-21
Mac Address parameter, 3-27
Max Age parameter, 1-27, 2-53
Max Name Cache Entries parameter, 3-16
Max number of RDs parameter, 2-40
Max Number Query Cache Entries parameter, 3-19
Max Translation Entries parameter, 4-18

Multicast addresses, 4-21

N

Name Cache Age parameter, 3-16
Name query frame, 3-3
Name recognized frame, 3-3
Names, NetBIOS, 3-1 to 3-9
Native Mode LAN
  access list, assigning to a port, 5-11 to 5-13
  enabling ranges for, 5-14
  implementation notes for, 5-3 to 5-4
  overview of, 5-1 to 5-3
  parameter defaults, A-8
  parameters. *See* the individual index entries
  traffic, controlling on a network trunk, 5-4
Native Mode LAN parameters
  Add Security Header interface parameter, 5-9
  CUG value interface parameter, 5-10
  Disable interface parameter, 5-9
  Range Enable parameter, 5-16
  Range End add security range parameter, 5-13
  Range Start add security range parameter, 5-13
  SAID Type interface parameter, 5-10
  SAID Value interface parameter, 5-10
  Security List Action interface parameter, 5-11
NetBIOS
  broadcast reduction, 3-4 to 3-9
  cache aging, 3-8
  cache lookup, 3-8
  client name caching, 3-5, 3-14, 3-21
  datagram, 3-4
  datagram RIF caching, 3-6, 3-15
  global parameters, editing, 3-13 to 3-19
  interface parameters, editing, 3-20 to 3-22
  names, 3-1 to 3-9
  query caching, 3-7, 3-18, 3-19, 3-22
  server name caching, 3-6
  session, establishing a, 3-3 to 3-4
  sessionless communication, 3-4
  statically configured clients and servers, 3-22 to 3-28
  used with DLSw, 3-10
NetBIOS parameters
  15-Character NetBIOS Name Caching, 3-15
  Create MIB Instances for Cached Name, 3-15
  Create MIB Instances for Cached Query, 3-18
  Enable, 3-27
  Hash Entry Count, 3-17
  MAC address, 3-25
  Mac Address static list, 3-27
  Max Name Cache Entries, 3-16
  Max Number Query Cache Entries, 3-19
  Name Cache Age, 3-16
  NetBIOS Client Name Cache, 3-14
  NetBIOS Datagram RIF Cache, 3-15
  NetBIOS Server Name Cache, 3-14
  NetBIOS Station Name, 3-25
  RIF from Router, 3-26
  RIF from Router static list, 3-27
Network Basic Input/Output System (NetBIOS). *See* NetBIOS
Network speeds, with translation bridge, 4-7
NML. *See* Native Mode LAN

O

Outbound STEs parameter, 2-41

P

Parameters. *See* Global parameters
Path cost, 1-10, 1-11, 1-32, 2-57
Path Cost parameter, 1-32, 2-57
Port
  cost, 1-10, 1-11
  identifier, 1-10
  priority, 1-10, 1-31
  root, 1-11, 1-32, 2-57
Priority parameter, 1-31
Protocols, translation bridge support, 4-7

Q

Query caching, 3-7

R

Range Enable (NML) parameter, 5-16
Range End (NML) parameter, 5-13
Range Start (NML) parameter, 5-13
RIF from Router parameter, 3-26, 3-27
RIF. *See* Routing information field
Ring ID
  for backbone IP network, 2-25
  mapped to IP address, 2-43
  of a LAN segment, 2-2
  of IP network, 2-37
  of source routing circuit, 2-41
  on ARE frame, 2-2
  with IP encapsulation, 2-5
Ring number, used with translation bridge, 4-3, 4-13, 4-17
Route information field database, 4-2
Routing information field (RIF), 2-5, 2-9, 3-26, 3-27, B-2

S

SAID Type (NML interface) parameter, 5-10
SAID Value (NML interface) parameter, 5-10
SAPS parameter, 4-20
Security List Action (NML interface) parameter, 5-11
Server name caching, 3-6
  disabling, 3-14
Session, establishing a NetBIOS, 3-3 to 3-4
Sessionless communication, in NetBIOS, 3-4
Source Route Explorer Type parameter, 4-20
Source route spanning tree parameters
  editing, 2-50 to 2-55
  Forward Delay, 2-55
  Hello Time, 2-54
  Max Age, 2-53
  Path Cost interface, 2-57
  Spanning Tree Enable, 2-51
  Spanning Tree Enable interface, 2-57
Source routing, 2-1 to 2-58
  across Token Ring networks, 2-11
  defaults, A-3, A-4
  disabling, 2-35, 2-40, 2-58
  enabling, 2-35, 2-40
  explorer frames, 2-11
  frame structure
    explorer frames, 2-13
    IP encapsulated frame, 2-19
    of a specifically routed frame, 2-16
  IP encapsulating bridge
    example of, 2-17
  on a circuit, 2-25
  over FDDI, 2-21
  over frame relay, 2-21
  route discovery, 2-11
  specifically routed frames (SRF), 2-14
Source routing bridge
  Conn. IP NTWK Ring Number global parameter, 2-37
  Enable global parameter, 2-35
  Enable interface parameter, 2-40
  Encapsulation Format, 2-43
  Frames with IP Ring interface parameter, 2-42
  global parameters, editing, 2-33 to 2-38
  Inbound STEs interface parameter, 2-42
  interface parameters, editing, 2-38 to 2-43
  IP Address interface parameter, 2-43
  IP Encapsulation global parameter, 2-37
  IP MTU Size global parameter, 2-38
  Max number of RDs interface parameter, 2-40
  Outbound STEs interface parameter, 2-41
  Source Routing Ring Number interface parameter, 2-41
  SR Bridge ID global parameter, 2-36
  SR Bridge Internal LAN ID global parameter, 2-35
  SR Group LAN ID global parameter, 2-36
  translation bridge operations, 4-3 to 4-4
  WAN Broadcast Address interface parameter, 2-43
Source Routing Ring Number parameter, 2-41

Source Routing Translate/Learning Bridge
enabling on a circuit, 4-12
Source routing-to-transparent translation bridge. *See* Translation bridge
Source-route endstations, 2-9 to 2-10
Spanning tree
defaults, A-2
disabling, 1-25, 1-31, 1-32
enabling, 1-25, 1-31
enabling over source routing, 2-51
interface parameters, editing, ?? to 1-32
service by transparent bridge, 1-1
Spanning tree algorithm, 2-3
configuring, 1-10 to 1-13
designated bridge for, 1-11
example of, 1-8 to 1-10
global parameters, editing, 1-24 to 1-29
root bridge for, 1-10
used with NetBIOS, 3-9
values needed by, 1-10
with translation bridge, 4-8 to 4-9
Spanning tree broadcast routing, 2-3
Spanning Tree Enable parameter, 2-51, 2-57
Spanning tree explorer (STE) frame, 2-3, 2-41, 4-3, 4-5
Spanning tree parameters
Enable, 1-25, 1-31
Forward Delay, 1-29
Hello Time, 1-28
Max Age, 1-27
Path Costr, 1-32
Priority interface, 1-31
Specific routing, 2-4
Specifically routed frame (SRF), 2-4, 4-4
Speed of network, with translation bridge, 4-7
SR Bridge ID parameter, 2-36
SR Bridge Internal LAN ID parameter, 2-35
SR Group LAN ID parameter, 2-36
SRF. *See* Specifically routed frame
Station type, 4-24 to 4-26
STE. *See* Spanning tree explorer (STE) frame
Support Source CD, xxiv

T

Token Ring Functional Address parameter, 4-23
Token Ring networks
source routing across, 2-11
Translation bridge
Aging Value global parameter, 4-18
Broadcast Conversion global parameter, 4-19
configuring, 4-11 to 4-12
creating a, 4-14
database aging mechanism, 4-2
databases for, 4-2
definition of, 4-1
disabling, 1-24, 4-17, 4-26
Enable global parameter, 4-17
enabling, 1-24, 4-14, 4-17
Ethernet MAC Address parameter, 4-25
Ethernet Multicast Address parameter, 4-23
Ethernet Type global parameter, 4-19
Ethernet Type parameter, 4-26
frame formats, 4-6
frame lengths, 4-6
global parameters, editing, 4-15 to 4-20
interfaces supported, 4-7
LAN speeds, 4-7
MAC address conversions, 4-21 to 4-23
MAC address formats for, 4-6
Max Translation Entries global parameter, 4-18
operations with ARE frames, 4-3 to 4-4
operations with SRFs, 4-4
protocols supported with, 4-7
SAPS global parameter, 4-20
Source Route Explorer Type global parameter, 4-20
station type, 4-24 to 4-26
Token Ring Functional Address parameter, 4-23
using a ring number, 4-3
Virtual LAN ID global parameter, 4-13, 4-17

Translation Bridge Enable parameter, 1-24

Translation services, transparent bridge, 1-2, 1-3 to 1-8

Transparent bridge
- as designated bridge, 1-11
- as root bridge, 1-10
- Bridge Table Size parameter, 1-21
- disabling, 1-20, 1-24, 1-32
- Enable Forwarding DB parameter, 1-22
- Enable global parameter, 1-20
- Enable interface parameter, 1-24
- enabling, 1-20, 1-24
- filters for, 1-14
- forwarding table. *See* Forwarding table
- global parameters, editing, 1-19 to 1-22
- interface parameters, editing, 1-22 to 1-24
- Translation Bridge Enable interface parameter, 1-24
- translation bridge operations, 4-4 to 4-5
- translation services, 1-3 to 1-8

Transparent-to-source routing translation bridge. *See* Translation bridge

V

Virtual Lan ID parameter, 4-13, 4-17

W

WAN Broadcast Address parameter, 2-43

World Wide Web, Bay Networks home page on, xxiii